Ocularis Administrator

User Manual

© 2014 On-Net Surveillance Systems Inc.

On-Net Surveillance Systems, Inc.
One Blue Hill Plaza, 7th Floor, PO Box 1555
Pearl River, NY 10965
Phone: (845) 732-7900 | Fax: (845) 732-7999
Web: www.onssi.com

Ocularis 4.1

00007142014-1133-4.1-.4.1.0.155

Legal Notice

This product manual is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

© 2002-2014 On-Net Surveillance Systems, Inc. All rights reserved. OnSSI and the 'Eye' logo are registered trademarks of On-Net Surveillance Systems, Inc. Ocularis, Ocularis Client, Ocularis Client Lite, Ocularis Video Synopsis, NetEVS, NetDVMS, NetDVR, ProSight, NetGuard, NetGuard-EVS, NetSwitcher, NetMatrix, NetCentral, NetTransact, NetPDA and NetCell are trademarks of On-Net Surveillance Systems, Inc. All other trademarks are property of their respective owners.

On-Net Surveillance Systems, Inc. reserves the right to change product specifications without prior notice.

US patent # 8,390.684 B2 for Ocularis Client

Patents Applied For in the U.S. and Abroad

Table of Contents

INTRODUCTION **1**

OVERVIEW **2**

PREREQUISITES **3**

OCULARIS ADMINISTRATOR **4**

OCULARIS ADMINISTRATOR LAUNCH 4
THE OCULARIS ADMINISTRATOR INTERFACE 5
Ocularis Administrator Tabs *5*
Ocularis Administrator Process Flow *6*
Server / Events Tab *7*
Servers Pane 7
NAT (Network Address Translation) 10
Servers List 12
Updating Servers 13
Selecting Licensed Cameras 15
CURRENT Expiration Notice 17
Camera Properties 18
Actions 23
Events Pane 34
Events Toolbar 35
Batch Handle Events 35
Purge Closed Events 36
Simple Event Rules 37
Event Properties 39
Event Retention 42
Composite Events 44
Data Link / Generic Events 47
Device Filter / Event Filter 53
Filter Lock 55
Users / Privileges Tab *56*
User / Privileges Toolbar 56
Working with User Groups 57
User Group Privileges 58
User Privileges 60
Device Privileges 64
Video Wall Privileges 69
Configuring a Video Wall 71
Views Tab *72*
Resizing Panes 73
View Basics 74
View Configurations 75
Contents 75
Content Navigation 76
View Organization 80
Creating Views 80
View Modification 84
Shared Views 85
Configuring View Content Types 88
Carousel Configuration 90
Hot Spot Configuration 95
Push Video Configuration 96
Web Configuration 97

Blank Screen Configuration 98
Assets Tab *99*
Maps 100
Map Icons 100
Event Audio Clips 101
Maps Tab *103*
Working with Maps 107
Linking Maps 111
Shortcuts and Pins *111*
Sharing Maps 116
EVENT MANAGEMENT 119
EVENT CONFIGURATION 120
Quick Reference – EVENTS 120
EVENT HANDLING 121
Table Management Tab *121*
Configure Classifications 122
Configure Tags 123
Configure Cases 124
Distribution Groups Tab *125*
Distribution Groups 126
Logs Tab *135*
Configure Auditing 135
Viewing the Audit Log 136
Exporting the Audit Log 141
About Tab *143*
About Ocularis 143
License Information 143
Help 144

APPENDIX 145

THE ONSSI EVENT COORDINATOR 145

CONTACT INFORMATION 146

Introduction

The **Ocularis Platform** consists of the following components:

- **Ocularis Base** – server software application which regulates and manages the flow of data between video client users, recording servers, video wall management, event management and alerting.
- **Ocularis Administrator** - The front end software application used to configure and manage Ocularis Base.
- **Ocularis Client** – OnSSI's award winning video client application used to view and monitor surveillance video.
- **Ocularis Recording Component** – Camera management and recording software. Each feature set of Ocularis contains a corresponding recording component application.
- **Optional Add-On Applications** – these currently include:
  - Remote VideoWall
  - Ocularis OpenSight™
  - Ocularis Media Server

Add-ons are made available as they are introduced. See our website www.onssi.com or call OnSSI Sales for information on Ocularis Add-Ons.

For all Ocularis features sets, configuration of Ocularis is performed using the *Ocularis Administrator* application.

This manual covers the component(s): **Ocularis Administrator**

For information on other components, please refer to the following documents which can be obtained from OnSSI Support:

Ocularis Installation & Licensing Guide
Recording Component User Manual
Ocularis Client User Manual
Ocularis Viewer User Manual

Overview

Ocularis is a distributed, video-centric, PSIM (Physical Security Information Management) software platform, which offers central event, user rights, video distribution and system management.

Ocularis supports:

- The ability for the user to view, manage and record video from an unlimited number of IP and non-IP video surveillance cameras at multiple sites.
- The management of short- and long-term video storage, and combine video with non-video alerts, resulting in automatic video delivery to subscribers of interest.
- The utilization of off-the-shelf hardware, and facilitates the integration of new technologies, thus combining the detection and distribution of video events with data and alerts received from a host of physical security and transaction systems.
- The use of separate or common networks, VLANS or switches for connecting cameras to the recording servers and video clients. This provides physical network separation between the camera and servers/clients.
- The use of VMware to run recording servers and client applications on virtual computers, servers, and networks.

Ocularis consists of the following software components:

- Ocularis Base – This component provides for:
    - system-wide management
    - user access
    - shared event management
    - alarm and event correlation
    - video access and distribution

  Ocularis Base regulates and manages the flow of data between video client users, connecting recording servers and integrated alerting application using an SQL database. This allows creating composite events from multiple detection systems; sharing resources between video client users; shared bookmarking and event handling among multiple users at multiple sites; and management of all user authorization data. The front end application used to manage Ocularis Base is the *Ocularis Administrator*.

- Ocularis Video Recorder Software – This component provides for video recording, camera management, and archiving configuration. The different feature sets of Ocularis support different recording components. For instance, Ocularis ES supports recording component RC-E.
- Ocularis Client – This award winning component is the user interface for accessing video, managing alerts and shared event handling, and observing Video Wall environments.
- Add-Ons and Integrated Applications – includes Remote Video Wall, Ocularis OpenSight, and Ocularis Media Server which includes Ocularis Mobile and Ocularis Web.

Prerequisites

Prior to using the *Ocularis Administrator* application, the following steps should be completed:

1. *Ocularis Base* server software should be installed.
2. The *Ocularis Base* license should be activated.
3. *Ocularis Administrator* software application files should be installed.

See the *Ocularis Installation & Licensing Guide* for instructions on all steps listed above.

Ocularis Administrator

The *Ocularis Administrator* is the software application used for configuring *Ocularis Base*. This includes the management of recorders and the configuration of users, groups, cameras, maps, events, and video walls. The *Ocularis Administrator* application is primarily used by system administrators. This application may be installed on any machine with connectivity to the Ocularis Base machine, or even the Ocularis Base machine itself. It may be installed on more than one computer.

Ocularis Administrator Launch

1. Launch *Ocularis Administrator*:
   - from the desktop icon
   - or from the Windows menu ***Start ➔ All Programs ➔ OnSSI ➔ Ocularis Admin***

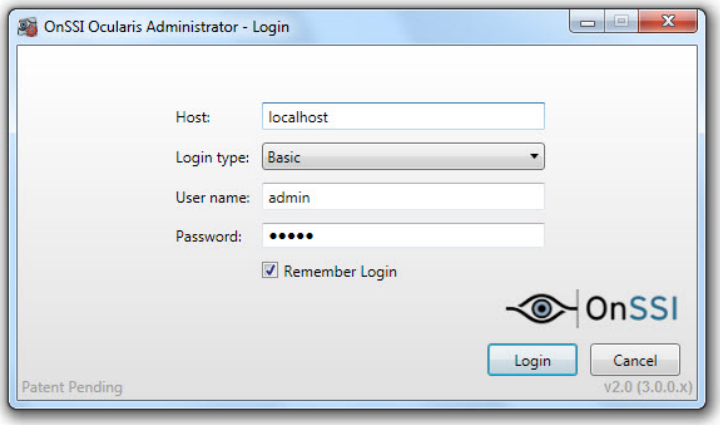


Figure 1 Ocularis Administrator Login Screen

2. Fill out the dialog based on the following:

Host	Enter the IP address where the Ocularis Base server software is installed. Using 'localhost' is acceptable if Ocularis Base is on the current machine. If the IIS port is anything other than 80, add ":port#" to the IP address.
Login type	Of the choices **[Current User]**, **Windows** or **Basic**, select **Basic** for first time use.
User name	Enter the user name for an account created with *Ocularis Administrator*. For first time access, enter the name: **admin**
Password	Enter the corresponding password for the user name entered. For first time access, enter the password: **admin**
Remember Login	Click this checkbox to have the application remember your login credentials for subsequent logins.
Version Number	The *Ocularis Administrator* software version number is located in the lower right portion of the Login screen.

3. When complete, click the **Login** button.

> ***Tip**: We recommend that you change the password for the Admin account immediately for security purposes. See* 'To Modify A User Account' *on page 62 for further instructions.*

> ***Note:** If you receive the following error message when logging in: "*An unsecured or incorrectly secured fault was received from the other party. See the inner FaultException for the fault code and detail*", check that the date and time on the PC with Ocularis Administrator is synchronized with the date and time on the PC with Ocularis Base.*

The Ocularis Administrator Interface

When you launch *Ocularis Administrator*, the resulting screen is a window comprised of a series of tabs.

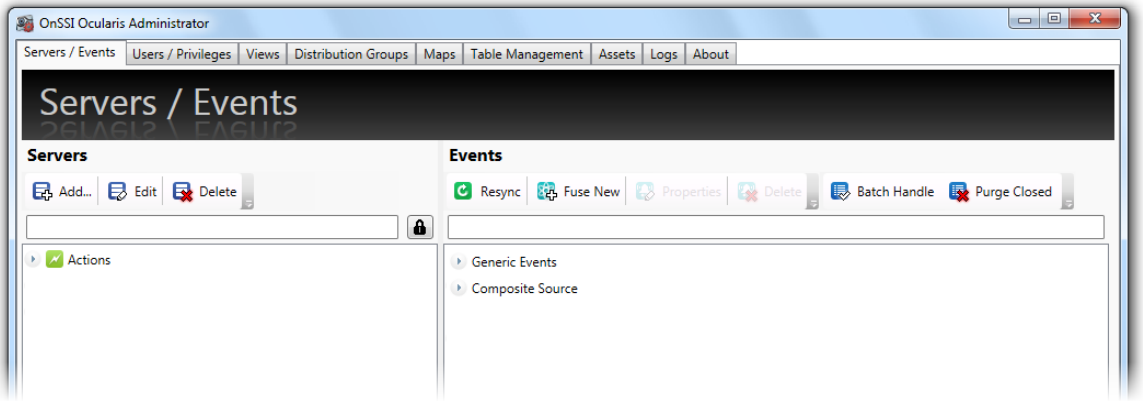


Figure 2 Ocularis Administrator Interface

Each tab serves to provide the system administrator with the ability to configure the various aspects of the video management system.

Ocularis Administrator Tabs

- Server / Events Tab
- Users / Privileges Tab
- Views Tab
- Distribution Groups Tab
- Maps Tab
- Table Management Tab
- Assets Tab
- Logs Tab
- About Tab

Ocularis Administrator Process Flow

A typical process flow for administrators to use when first configuring the system with *Ocularis Administrator* is as follows:

1. Import system recorders using the Server / Events Tab.
2. Create users and groups and assign device privileges in the Users / Privileges Tab.
3. Create views for the user groups in the Views Tab.
4. Enable and configure the Audit Log in the Logs Tab.
5. Import maps, icons and sound files in the Assets Tab.
6. Configure maps with cameras and views for use in video walls in the Maps Tab.
7. Create video wall names and assign video wall privileges in the Users / Privileges Tab. (for Ocularis ES, LS, CS and IS only)
8. Identify events and cameras you would like to monitor in the Server / Events Tab.
9. Identify the alert distribution and actions for system configured events in the Distribution Groups Tab.
10. Configure tags, classifications and cases in the Table Management Tab. Tags, classifications and cases are used when handling events and saving bookmarks.

Server / Events Tab

This tab is used to manage recorders, servers and events within the Ocularis environment.

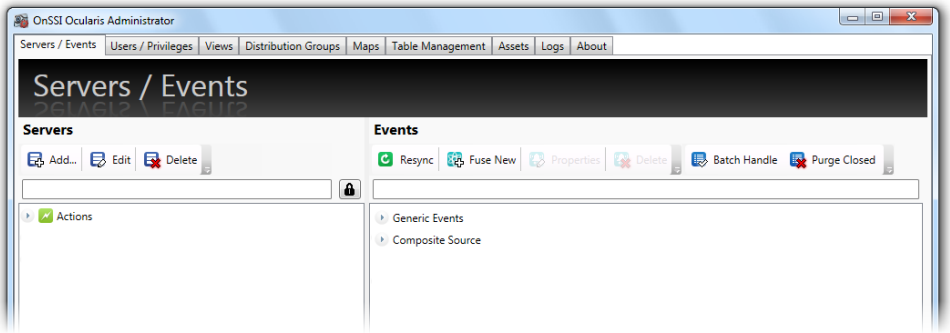


Figure 3 Servers / Events Tab

The tab contains two panes: **Servers** and **Events**. Administrators identify various servers used in the system, including recording components (NVRs), in the left pane and configure events in the right pane.

Servers Pane

Configuration and information from existing recorders and servers to be used with Ocularis need to be imported into the *Ocularis Administrator*. This is done within the **Servers** pane of the **Servers / Events** Tab.

Servers Toolbar

The toolbar in the **Servers** pane of the **Servers / Events** Tab controls server related functions.

Figure 4 Servers Pane Toolbar

Adding a Server

To add a recording component, other server or supported camera with embedded NVR to Ocularis Base, follow these instructions. The OnSSI recorder that you may add is determined by the Ocularis SLC video channel licenses purchased. You may mix and match recorders in Ocularis Base for the same level of Ocularis or lower. For instance, if you have Ocularis CS, you may add an RC-C, RC-I or RC-P NVR to Ocularis Base. Add a camera with embedded NVR (e.g. Axis Camera Companion supported camera) here as well and it will appear as a one camera NVR. The amount of cameras with embedded NVRs that you can add is also controlled by the number of Camera NVR licenses purchased.

1. In the **Servers / Events** Tab, click the **Add** button.

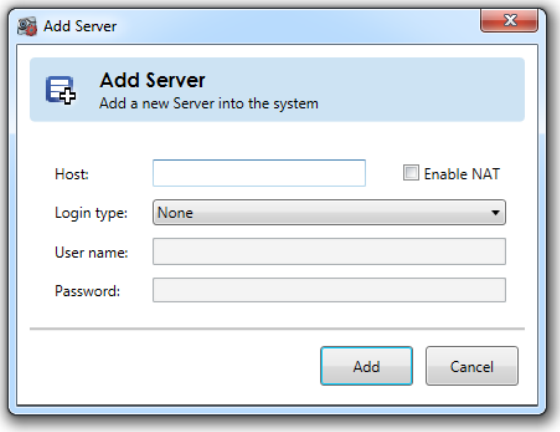


Figure 5 Add New

2. In the **Host** field of the resulting pop-up window, enter the IP Address and port number of the server or camera with embedded NVR to be added to the Ocularis Base system.

   - If the port number for the recorder or camera is 80, there is no need to enter it.
   - If the port number for the recorder or camera is a value other than 80, use the following format:

     IP Address:Port Number

   For example:

IP Address of Server:	192.168.10.111
Port for recorder:	8080
Enter:	**192.167.10.111:8080**

3. If NAT is used due to one or more components requiring access from outside the firewall, click the *Enable NAT* checkbox and see *To Configure NAT Servers* on page 10.

4. Select the **Login type** from the drop-down. Choose from **Basic** or **Windows** based on an account located on the recording component that has full access rights.

   ***Note:** For Ocularis ES and Ocularis LS you must use a Windows account on the Management Server to import into Ocularis Base.*

   ***Note:** For cameras with embedded NVRs, select **Basic** login type.*

5. Enter a **User name** for the corresponding user account.

   ***Note:** It is important to use an account on the recorder or server with **full administrative access**. Only one account on the recording component is necessary when using Ocularis Base.*

   ***Note:** For cameras with embedded NVRs, enter the user name configured on the camera. The user name is case sensitive.*

6. Enter the **Password** for the username entered. The password is case sensitive.

7. Click **Add**.

The recorder/server or camera with embedded NVR should now appear in the list. Repeat this process for each recording component to be added to the system.

> ***Note:*** *if the recorder you are importing has more cameras than your Ocularis license allows, you will receive a warning message that the number of cameras exceeds the amount licensed.*

Cameras with embedded NVRs

Cameras with embedded NVRs appear in line with other NVRs in the Servers pane. Expand these for the corresponding camera, microphone and triggers. Cameras with embedded NVRs require a special license. Only video for these cameras are supported at this time. Use this camera as you would any other in Ocularis (e.g. create an alternate camera name, use in a view, create a privacy mask, etc.)

For *Editing a Server*, see page 14.
For *Deleting a Server* see page 14.

NAT (Network Address Translation)

If video will be accessed from computers outside the firewall of the Ocularis Base machine, or if recorders are located on networks also outside of the Base network, NAT must be configured.

TO CONFIGURE NAT SERVERS

1. In the **Servers / Events** Tab, click the **Add** button.
2. In the *Add Server* pop-up, check the **Enable NAT** checkbox.

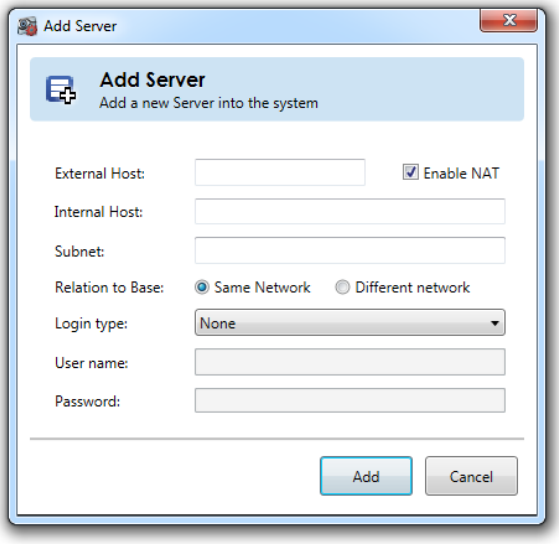


Figure 6 Add Server with NAT

3. Fill in the NAT fields as follows:

External host	Enter the public IP address as defined on the network firewall. Append the IP address with **":port #**"
Internal Host	Enter the internal IP address of the recording server including "**:port #**" after the address. This port number may be the same used in the External host address.
Subnet	Identifies the local subnet(s).
Relation to Base	**Same Network** – Use this option when the recorder machine is on the same network as the Ocularis Base machine. **Different Network** – Use this option when the recorder machine is on a different network as the Ocularis Base machine or resides outside the firewall.
Login type	Choose Basic or Windows based on the user account set up on the recorder that you will be using to add the recorder.
User name	Enter the user name for a user account on the recorder. In most cases, add an account with full administrative privileges.
Password	Enter the password for the corresponding user account.

4. When the *Add Server* pop-up is completed, click **Add**.

The following is an example of how two different recorders might be configured via NAT.

When to use NAT (Network Address Translation)

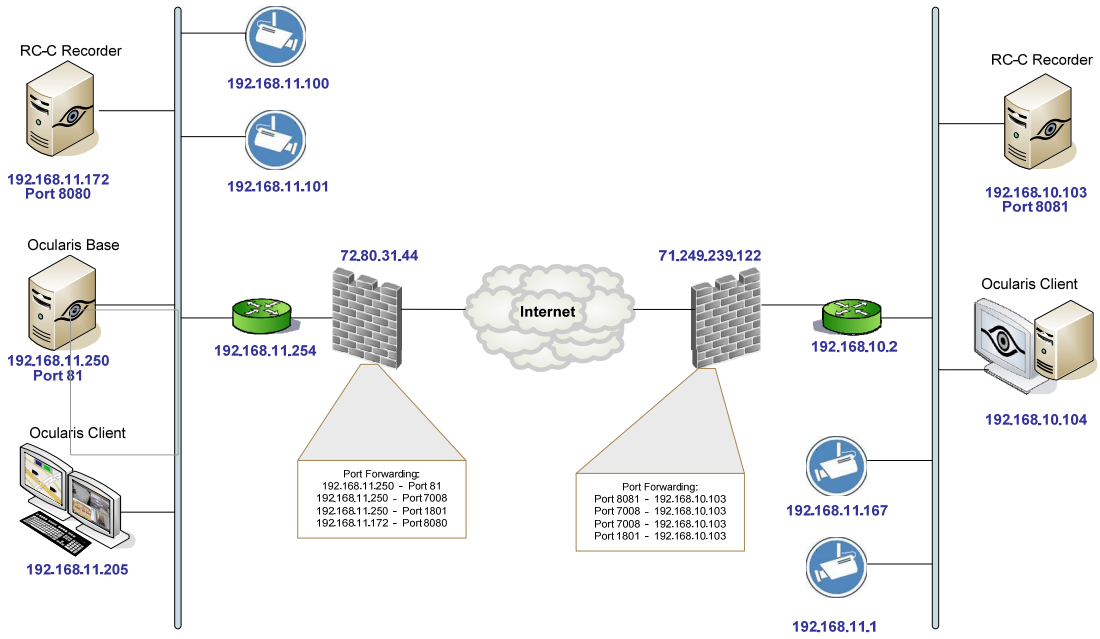


Figure 7 Sample Environment+

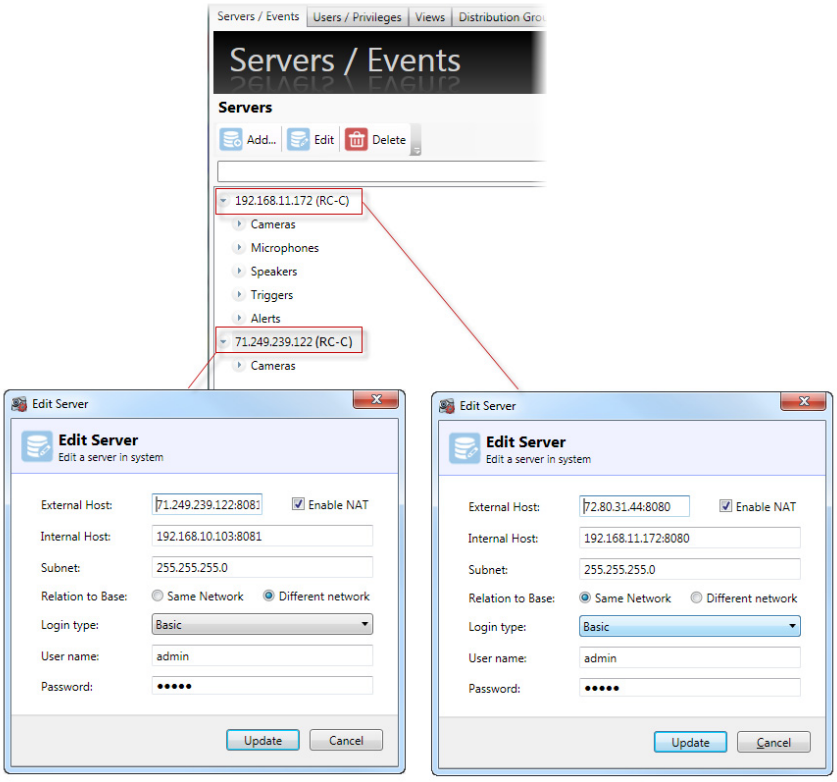


Figure 8 Sample NAT Configurations

Servers List

As recording servers are added to Ocularis, the resulting **Servers** list is collapsible and expandable by clicking the symbol in front of the list item. Cameras, Triggers, Microphones, Speakers, Relay, Alerts and Inputs are imported from the recorders as shown in Figure 9 .

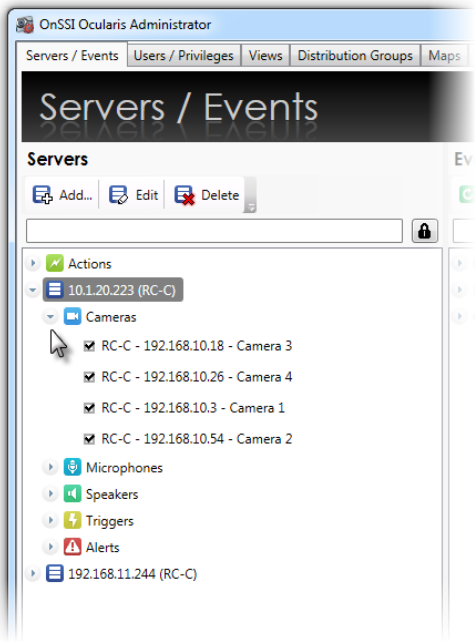


Figure 9 Added Recorders

The recording component is displayed by its IP address followed by the type of recording component (e.g. RC-C). If you imported a camera with corresponding NVR (such as a camera managed by the Axis Camera Companion), the device will be listed at the same level as other servers. Expand the node to view the camera name and license checkbox.

> ***WARNING***:
> *The camera names listed here are those assigned in the recording component. Please note that certain special characters are not supported by Ocularis and if included in a device name, may cause erratic or non-functional behavior. We recommend you avoid all special characters in camera names and events including (but not limited to):*
>
> **< > & ' " \ / : * ? | [ ]**

Updating Servers

In the course of normal use, recorder properties change over time. New cameras are added, outdated cameras are removed, camera settings are changed, events are implemented, software is upgraded, etc. In order for Ocularis be aware of any new parameters configured on the recorder, the recording component (RC) server information should be updated periodically. When you upgrade recording component software, you should always refresh the server in Ocularis Administrator.

To Update a Server's Configuration

Follow these steps to update recorder configuration and camera list. Use this function when you add or remove cameras or modify camera settings. This procedure is not to be used to modify the recorder's IP Address. (See *Editing a Server* below.)

1. In the **Servers / Events** Tab, right-click the server you wish to update from the **Servers** pane.
2. In the resulting menu, select 'Refresh server'.

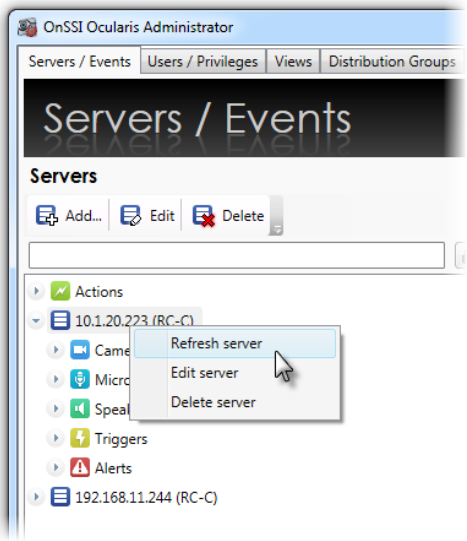


Figure 10 Right-click to Refresh the server

An "Updating" message appears as the configuration is refreshed from the selected server. Device licensing is updated.

> ***Note: Licensing change in Ocularis 4.1 Recorders***
>
> The recorders included with v4.1 have been optimized to reduce the amount of licenses needed for encoders and multi-lens cameras. Whereupon previously you needed 1 license per stream, with these recorders you now only need 1 license per IP address on the device. Supported recorders include: RC-P 2.6, RC-I 8.6, RC-C 8.6, RC-L 7.0 and RC-E 7.0.
> If you have these recorders, use the 'Refresh Server' function after you upgrade the recorder in order to update the license distribution. You may find that you have extra licenses using this new model. Older version recorders have not changed in that you will need 1 license per stream.

3. Verify the license application by expanding the recording component. Licensed devices appear with a checkmark. Re-apply licenses if necessary.
4. Repeat these steps fro each server you wish to update.

Editing a Server

Follow these steps to modify a recorder's IP Address or changes to its corresponding username and password.

TO EDIT A RECORDER'S IP ADDRESS OR ACCOUNT INFO

1. In the **Servers / Events** Tab, select the server you wish to update from the **Servers** pane.
2. Either right-click the server and select 'Edit server' or click the **Edit** button in the Servers Toolbar.

   An *Edit Server* pop-up screen appears.

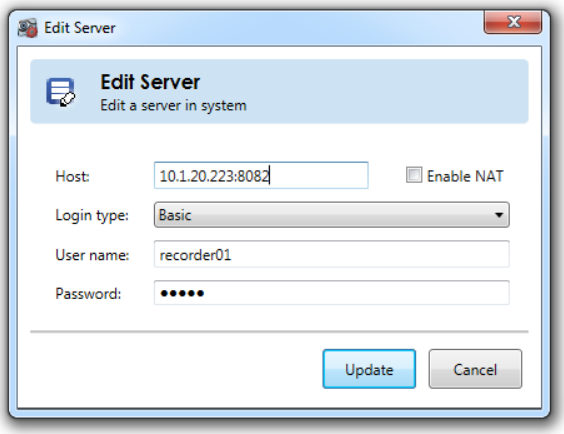


Figure 11 Edit Server Sample

3. Modify the settings as needed.
4. Click the **Update** button.

   An "Updating" message appears as the configuration is updated.

Deleting a Server

Use the procedure below to remove a recorder or other server from the Ocularis Base. This will not delete the recorder or its software; it will simply remove Ocularis' access to the server. This function is only available to the **admin** user of *Ocularis Administrator*. 'Group Administrators' do not have permission to delete servers.

TO REMOVE A RECORDER OR OTHER SERVER

1. In the **Servers / Events** Tab, select the server you wish to remove from the **Servers** pane.
2. Either right-click the server and select 'Delete server' or click the **Delete** button in the Servers Toolbar.

   A message appears as the server is removed.

Selecting Licensed Cameras

In the Servers pane, you may expand the recorders in order to see the imported cameras associated with each one. A checkbox appears next to each camera, indicating if the camera is Ocularis licensed or not.

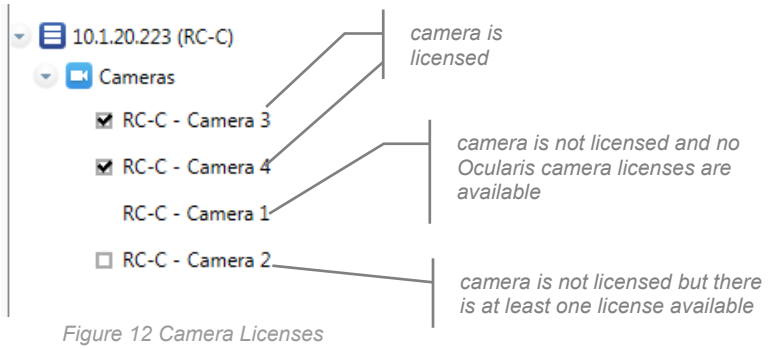

10.1.20.223 (RC-C)
Cameras
RC-C - Camera 3
RC-C - Camera 4
RC-C - Camera 1
RC-C - Camera 2
camera is licensed
camera is not licensed and no Ocularis camera licenses are available
camera is not licensed but there is at least one license available

Figure 12 Camera Licenses

Ocularis camera licenses are purchased as part of the Ocularis feature set licensing. You may view the quantity of Ocularis camera licenses in the *License Information* section of the **About** Tab. Cameras which are 'unchecked' or show no checkbox are not licensed and will not be available for use with Ocularis. You must either purchase additional Ocularis camera licenses or reassign the camera selection.

TO REASSIGN CAMERA SELECTION

If you need to reassign camera selection for licensed cameras, follow these steps:

1. In the **Servers / Events** Tab, expand the recorder and Cameras node accordingly.
2. Then, deselect a camera which you want to unassign. Do this by unchecking the adjacent checkbox.
3. When a camera license is deselected, unassigned cameras become available for selection and empty checkboxes appear.
4. Click the checkbox for each camera you wish to be used with Ocularis. If the checkboxes disappear, you have used up all available Ocularis camera licenses.

Multi-Channel Device Licensing

With the introduction of Ocularis v4.1, the number of licenses required for certain devices has been reduced. In prior versions, one Ocularis license is required for each video stream. In v4.1, one license is required for each IP Address on a device. This licensing model applies to video encoders and multi-lens cameras on the following recording component versions: RC-P 2.6, RC-I 8.6, RC-C 8.6, RC-L 7.0 and RC-E 7.0. If you have Ocularis v4.1 with older version recorders, the older license model still applies.

For instance, the example shown in Figure 13 shows a camera with four lenses (Arecont 4 channels) and a video encoder with four channels (Axis M7010) on Ocularis v4.1 with RC-I 8.6. As you can see, only two Ocularis licenses are used for these eight channels. If RC-I 8.5 was used, you would require eight Ocularis licenses. Verify your license counts in the About tab. The six extra licenses may now be applied to additional cameras/devices.

Update the camera license counts after the recording component upgrade is complete by right-clicking the component name in the **Servers / Events Tab** and clicking 'Refresh Server'.

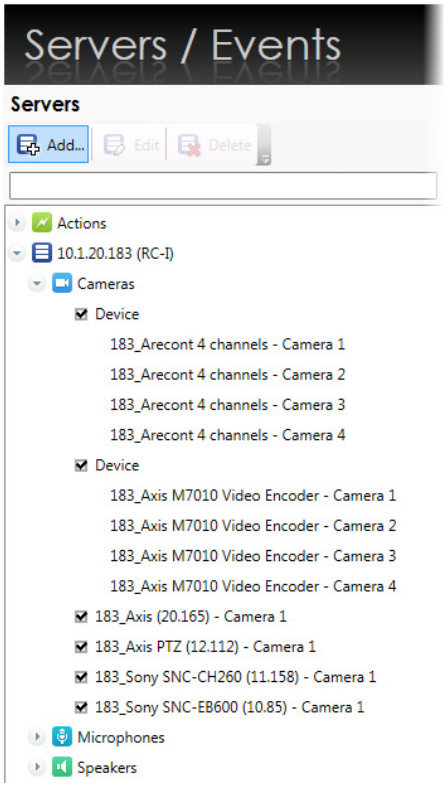


Figure 13 Multi-Channel Devices in v4.1

You can, however, still use each stream individually for blank screen events, assigning privileges, views and maps. With this licensing model, if you uncheck (unlicensed) the device, all channels/streams on that device become unlicensed.

> ***Note**: The device name for multi-lens cameras and encoders for RC-P 2.6, RC-I 8.6 and RC-C 8.6 recording components will appear in the Servers / Events Tab as 'Device'. With RC-L 7.0 and RC-E 7.0, the device name will be inherited from the recording component itself.*

CURRENT Expiration Notice

StayCURRENT is OnSSI's program designed to keep your Ocularis software up-to-date. Under StayCURRENT, your organization has access to all upgrades of Ocularis. (see (http://www.onssi.com/sales/current-program) for more information on StayCURRENT).

The Ocularis Administrator application displays a pop-up 'Notice' box to inform all administrators about the status of their StayCURRENT plan. The following rules apply:

- If the expiration date for the StayCURRENT plan is further than 90 days out, no indication pop-up appears inside Ocularis Administrator. The expiration date can be found on the **About** tab.
- If the expiration date for the StayCURRENT plan is 90 days in the future (or sooner), a yellow 'Notice' pop-up appears identifying the expiration date.

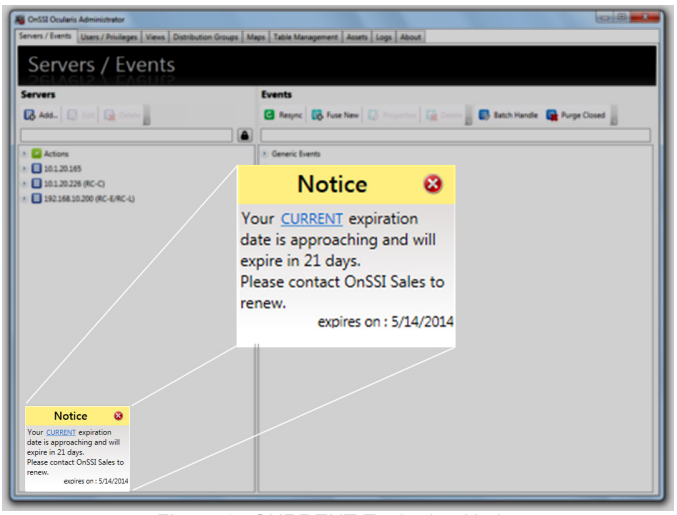
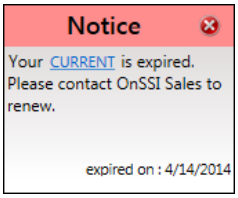

Servers / Events
Servers
Events
Notice
Your CURRENT expiration date is approaching and will expire in 21 days.
Please contact OnSSI Sales to renew.
expires on : 5/14/2014

Figure 14 CURRENT Expiration Notice

- If the expiration date for the StayCURRENT plan passes, a red 'Notice' pop-up appears. This pop-up will continue to appear for 14 days and then disappear completely.



The message is informational only. The software will continue to function beyond the StayCURRENT expiration date. You will not, however, be able upgrade to a newer version of Ocularis until the StayCURRENT expiration date has been extended. Click the CURRENT link to open the OnSSI corresponding webpage for information on StayCURRENT or contact OnSSI Sales to extend the expiration date.

The 'Notice' message will appear on each tab of the application. Click the 'Notice' bar to expand or collapse the message. Click the 'X' to clear the box for the current session. If still applicable, the message will appear again the next time you log in to Ocularis Administrator.

> ***Note**: Your StayCURRENT plan must be active to upgrade to major (e.g. 4.0 to 5.0) or minor (e.g. 4.0 to 4.1) releases of Ocularis. Service packs and fixes are available regardless of StayCURRENT status.*

Camera Properties

Certain parameters can be set on a camera by camera basis by the administrator in the **Servers / Events** tab. This is done by right-clicking a camera name in the *Servers* pane and selecting *Properties* (or double-click the camera name).

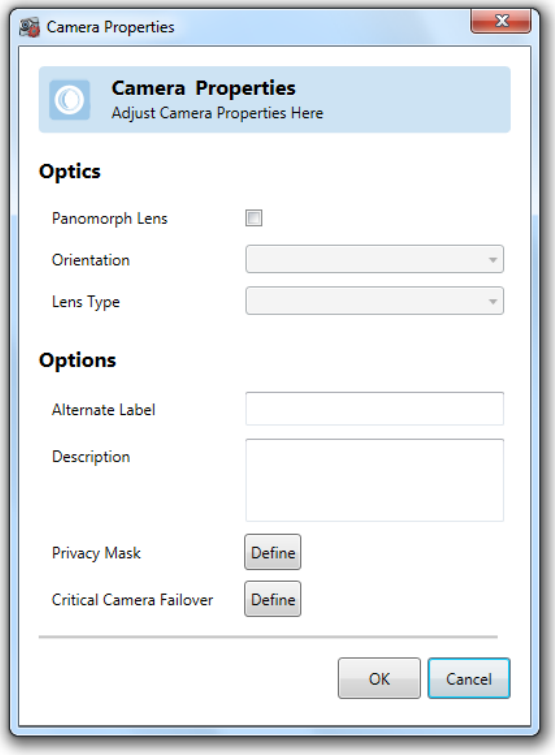


Figure 15 Camera Properties

Optics

In order to take advantage of Immervision's 360° panomorph lenses, the camera with the panomorph lens needs to be configured in the *Ocularis Administrator*.

1. Click the *Panomorph Camera* checkbox.
2. Select where the camera with the panomorph lens is installed under *Orientation*. Choices are: Ceiling, Wall, Floor
3. Select the lens under *Lens Type*.

The user will now be able to take advantage of the 360° x 180° field of view provided by the special lens when viewing via Ocularis Client.

Options

The following table describes additional parameters in the *Camera Properties* dialog box.

Item	*Description*
Alternate Label	The text entered here will be used to identify this camera in Ocularis Client. This gives the administrator the ability to change the display of a camera name without changing it permanently on the recorder. You may consider using this field in conjunction with Description (below) to clearly identify your cameras.
Description	You may add a description for the camera which provides more detail on its location, purpose, settings, etc. This field is available to administrators while viewing the camera thumbnail in preview modes within Ocularis Administrator as well as in tool tips within Ocularis Client. You may consider using this field in conjunction with Alternate Label (above) to clearly identify your cameras.
Privacy Mask	Click **Define** to identify areas on the video image to be masked for privacy. Only applicable to fixed cameras. See *Privacy Mask* below for more information.
Critical Camera Failover	Click **Define** to configure failover cameras for this camera. See below for more information.

Privacy Mask

A *Privacy Mask* is an area of an image that is blocked out from view. For instance, in an office environment you may want to see the images of the general office area but want to block out someone's private desk area to provide the employee with some privacy. In this example, you may select a section of the image to NOT appear in the video feed. This is called a privacy mask. Privacy masks may be used for legal or liability reasons as well.

Ocularis supports three levels of privacy masking: on the camera, on the recorder and within Ocularis. Setting a privacy mask in Ocularis has the following benefits:

- You may designate multiple but separate masks on the same image.
- The mask shapes can be any polygon. There are no shape restrictions.

Privacy Masks set in Ocularis are supported on fixed cameras only.

TO CREATE A PRIVACY MASK

1. In the **Servers / Events** tab, locate and right-click the desired camera.
2. Select **Properties**.
3. Click **Define** in the *Options* section of the *Camera Properties* pop-up.
4. In the *Draw Privacy Mask* pop-up, the camera image appears.
5. Use your mouse to identify an area or areas of the image that you wish to block out.

Figure 16 Right-click to draw privacy mask

To draw the area, right-click the mouse, drag, right-click, drag, repeat until you have identified the blocked area. Be sure to right-click back on the original starting point to complete the shape.

You may draw multiple, non-contiguous shapes.

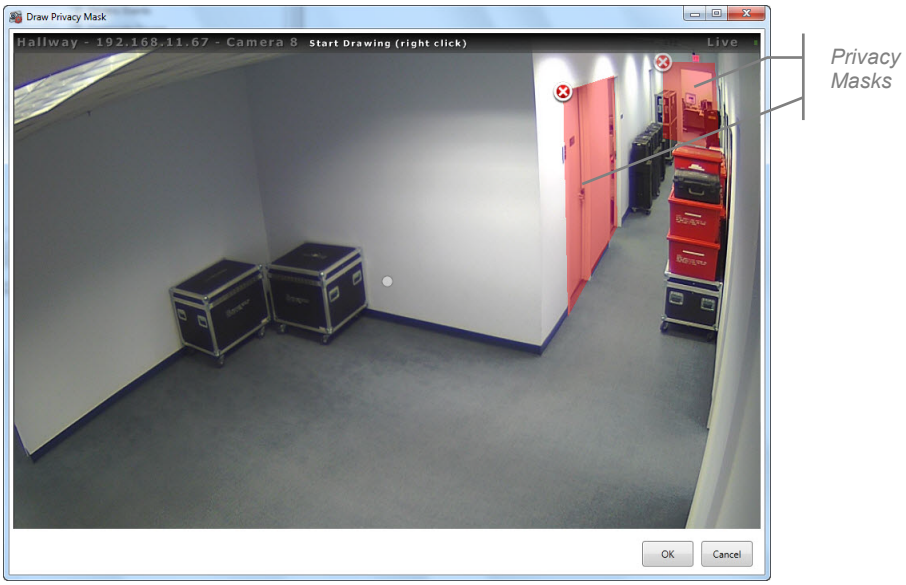


Figure 17 Configuring Multiple Privacy Masks

6. Click OK when finished setting the privacy mask(s).

   The mask shapes appear translucent on this screen to aid you in understanding what the mask is covering. When viewing video from this camera in a client, the shapes will be opaque.

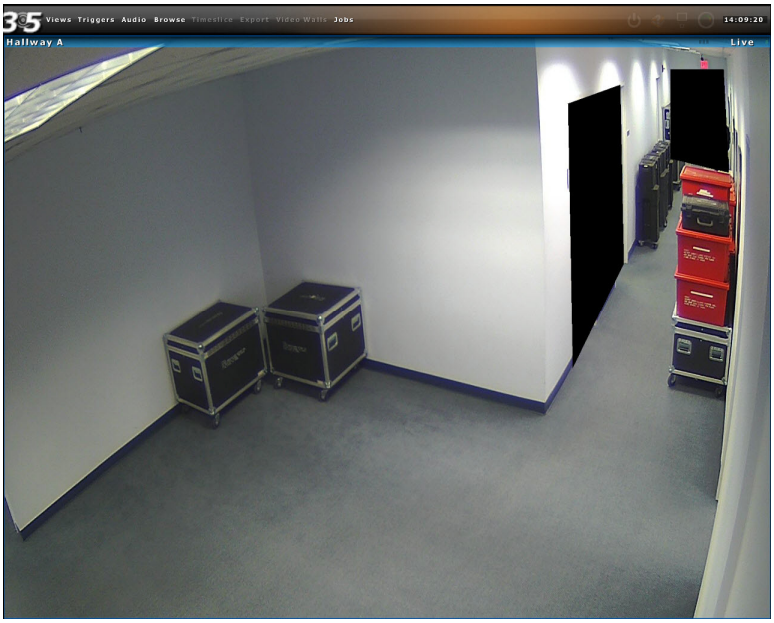


Figure 18 Privacy Masks when viewed in Ocularis Client

Critical Camera Failover

Critical Camera Failover is used for mission critical applications where live video cannot be interrupted. Camera streams may become unavailable for multiple reasons such as network failure, device failure or even recorder failure. Critical Camera Failover automatically switches the camera pane to an alternate stream in a little as 2-3 seconds without operator intervention and works in all Camera Views, Map Views and Alerts. Critical Camera Failover will continue to function even if Ocularis Base is unavailable. Multiple cameras can be designated as failover cameras for the same primary camera.

Cameras selected as failover cameras include:

- Duplicate camera stream from a redundant recorder
- Different camera from the same recorder
- Different camera from a different recorder
- Any combination of the above

TO CONFIGURE CRITICAL CAMERA FAILOVER

1. From the *Servers* pane, right-click the critical camera you wish to configure and select **Properties**.
2. In the 'Camera Properties' pop-up, click the **Define** button next to 'Critical Camera Failover'. The *Critical Camera Failover Editor* appears.

   The primary camera that you're setting up is listed at the top of the pop-up.

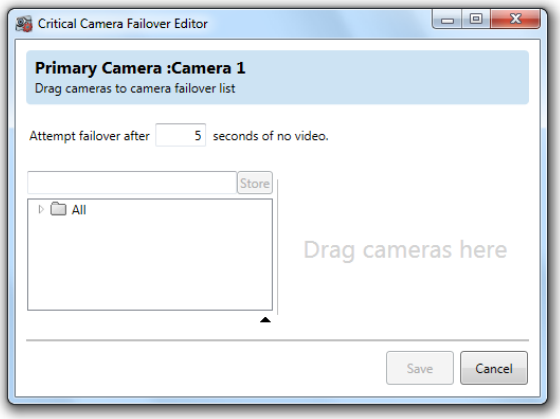


Figure 19 Critical Camera Failover Editor

3. Expand the camera folder(s) to expose the list of available failover cameras.

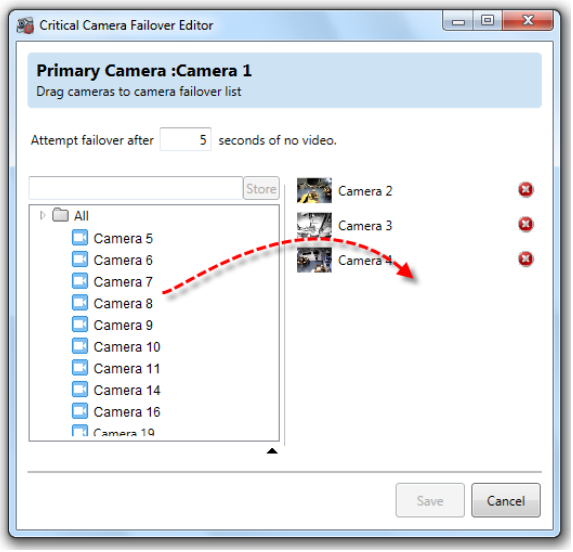


Figure 20 Drag and Drop to create failover cameras list

4. Drag and drop the desired failover camera(s) from the list on the left to the drop area on the right. There is no limit to the number of cameras that can be configured as a backup.

How Does It Work?

If the primary camera stream fails for any reason, the next camera in the list will be displayed in its place in the Ocularis Client. This could be in a view pane or on a map or video wall. If that camera fails then the next camera (in order) will appear. In the example above, if Camera 1 fails, Camera 2 will be displayed. If Camera 2 fails, Camera 5 will display. Then if Camera 5 fails, Camera 3 is displayed.

Ocularis Client monitors the stream and if it determines that the stream is no longer there, it will switch to the next camera in the list. The amount of time to wait to determine if the stream is live is controlled by the 'Switch Time' field when you configure the failover cameras. The more critical the camera, the shorter duration to use in this field.

When a failover camera is displayed in a view, there is a 'Failover Camera' overlay that appears in the view pane to notify you that the stream has changed. By default, the overlay is displayed for 10 seconds and then disappears. This time may be modified in the Client Setup of the Ocularis Client. The failover camera name is shown in the image bar of the pane along with an orange status light.

Also, when you use the mouse to display the pane's streaming information, you'll see a message that the video is a failover for the primary camera.

Lastly, during the time that the failover camera is displayed, Ocularis Client continues to check the primary camera stream. If the primary camera stream is restored, the video from this camera will be returned to the display.

The order of the cameras listed will be the order to display each failover camera. If you need to recorder the list, simply drag and drop cameras from within the list.

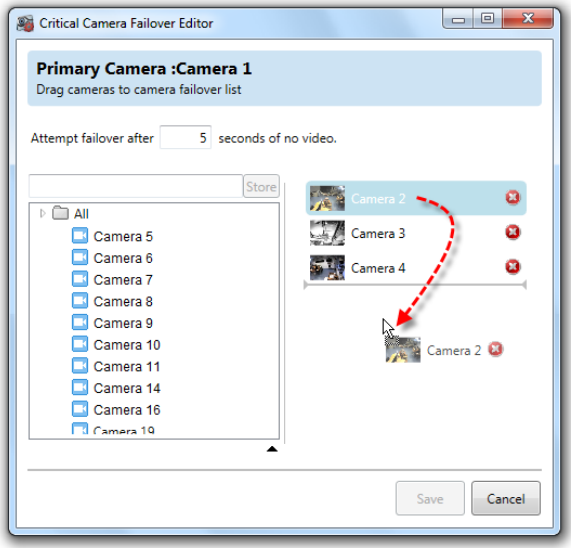


Figure 21 Drag and drop cameras to reorder the failover list

5. If you need to remove a camera from the failover list, simple click the red icon to the right of the camera name.
6. When finished configuring this camera's failover list, click **Save**. Then click **OK**.

Actions

One of the primary features of Ocularis is its ability to alert the right person when some event occurs. The alert can take several forms:

- Video from one or more cameras can appear on a dedicated monitor or portion thereof
- A custom sound can be played to alert an operator to a specific event
- A PTZ camera can be moved to a configured preset position
- An email can be sent to one or more people
- An HTTP Get or Post Request can be issued
- An outgoing data packet (generic string) can be sent

The first two items in the list above are configured in the Events pane and covered in the next section. The latter four items are configured in the Servers pane and discussed below.

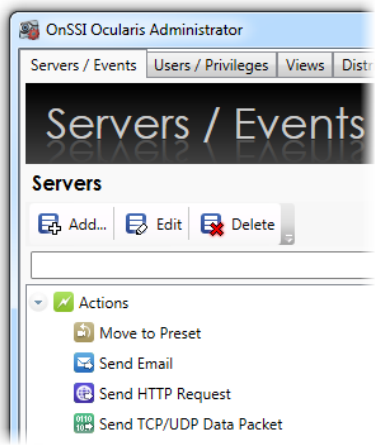


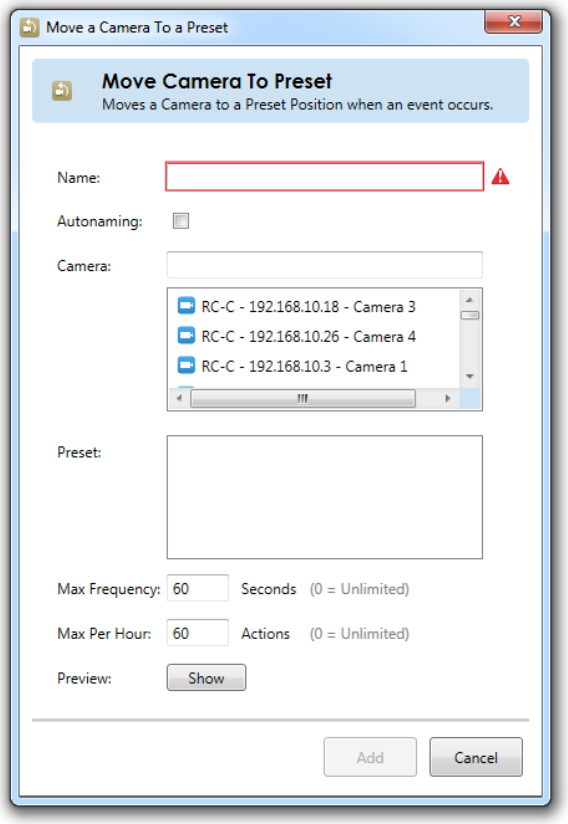
Figure 22 Alert Actions

Move to Preset

When a particular event occurs, one of the actions that you may configure is to move a camera to a preconfigured preset position. For instance, if there is an 'access denied' event received from a key card entry system, you may want a local camera to move to the position that views the door to see the incident as it occurs. The preset configurations are made under the actions. Associating the action with an event is done in the **Distribution Groups** tab. As a reminder, presets are set on the recording component using the Management Application (for PS, IS and CS) or the Management Client (for LS and ES). The presets are imported into Ocularis when the server is imported or refreshed in the **Servers / Events** tab.

To Add a New Preset Move

1. Expand the Actions node in the **Servers / Events** tab.
2. Right-click the 'Move to Preset' list item and select *Add New Move to Preset…*


Move a Camera To a Preset
Move Camera To Preset
Moves a Camera to a Preset Position when an event occurs.
Name:
Autonaming:
Camera:
RC-C - 192.168.10.18 - Camera 3
RC-C - 192.168.10.26 - Camera 4
RC-C - 192.168.10.3 - Camera 1
Preset:
Max Frequency: 60 Seconds (0 = Unlimited)
Max Per Hour: 60 Actions (0 = Unlimited)
Preview: Show
Add
Cancel

3. In the **Name** field, enter a descriptive name to identify this action. Alternately, if you click the **Autonaming** checkbox, the **Name** will be filled in automatically using the format:

   Move **[camera name]** to **[Preset name]**

4. Select the camera with the preset you wish to use in the action. You may use the **Camera** text field to filter the list by entering all or a portion of a key word within the camera name.

5. Once the camera is selected, configured presets appear in the **Preset** text field. Select the preset you wish the camera to move to once the event is configured.

6. The **Max Frequency** field is set to 60 seconds as the default value. This field identifies the time interval in seconds in which you would like to monitor alerts. This feature will reduce the amount of repeated alerts within a specified timeframe. You may modify this value to any number between 1 and 3600. A zero value indicates an unlimited time period and may accumulate many unnecessary events.

7. The **Max Per Hour** field allows you to control the maximum number of times you want this action to be performed in an hour.

8. Click the **Show** button to launch a pop-up that shows the image of the preset to insure that you are selecting the correct one. Click OK to close the Preview pop-up.

9. When done, click the **Add** button.

The preset move has just been configured but has not been assigned to any particular alert. This association is done in the **Distribution Groups** tab. See *Actions* on page 129.

Once a preset move has been configured, you may test, edit or delete the configuration.

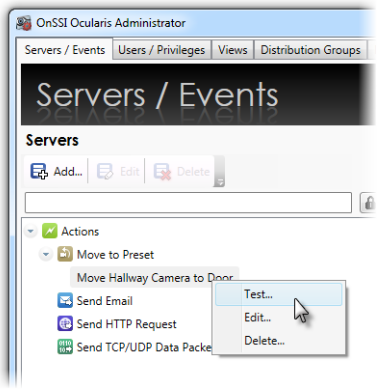


Figure 23 Preset Move Actions

To Test a New Preset Move

You can test the functionality of a configured preset move to be sure that it works properly.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Move to Preset** item.
3. Right-click the configured move to preset list item and select *Test…*
4. A pop-up appears indicating that a test move will be issued.
5. Click **Send** to execute the move.

To Edit a Preset Move

You can edit the configuration of a preset move if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Move to Preset** item.
3. Right-click the configured move to preset list item and select *Edit…*
4. Modify the changes as needed.
5. Click **Update** to save changes.

To Delete a Preset Move

You can delete a configured preset move if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Move to Preset** item.
3. Right-click the configured move to preset list item and select *Delete…*
4. An '*Are you sure you want to delete…*" pop-up is displayed. Click **Yes** to confirm the deletion.

Send Email

When an event occurs you may want to send an email to someone for notification purposes. Emails are configured in the **Servers / Events** tab and associated with an event in the **Distribution Groups** tab. An email SMTP server is required in order to send outgoing email.

To Configure an Email Server

Configuring your email server need only be done once.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Right-click the 'Send Email' list item and select *Configure Email Server…*

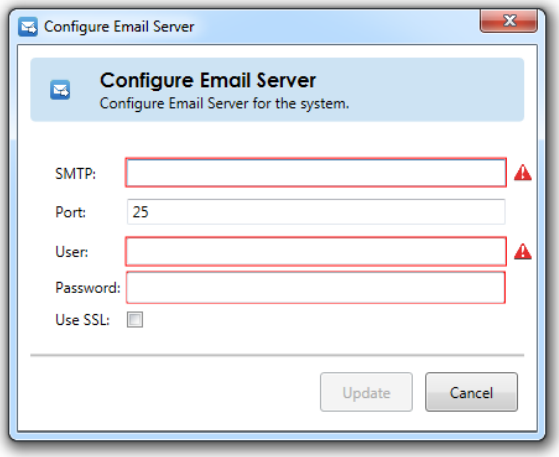


Figure 24 Configure the Email Server

3. Fill out the fields of the pop-up according to the following:

Item	***Description***
SMTP	Enter the host name for the SMTP email server.
Port	Identify the port number to be used to send email. Typically, port 25 is reserved for this but you can modify the port if necessary.
User	Enter the user account to be used as the sending email account.
Password	Enter the password for the user account.
Use SSL	Click this box if email server uses SSL (Secure Sockets Layer)

The red outlined warnings will disappear once data is entered in the correct format into each field.

4. When complete, click **Update**.

To Modify an Email Server Configuration

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Right-click the 'Send Email' list item and select *Configure Email Server…*
3. Modify the fields of the pop-up as needed.
4. When complete, click **Update**.

To Configure an Email

One or more emails can be pre-configured so that when an event triggers, a custom email can be sent.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Right-click the 'Send Email' list item and select *Add New Email…*

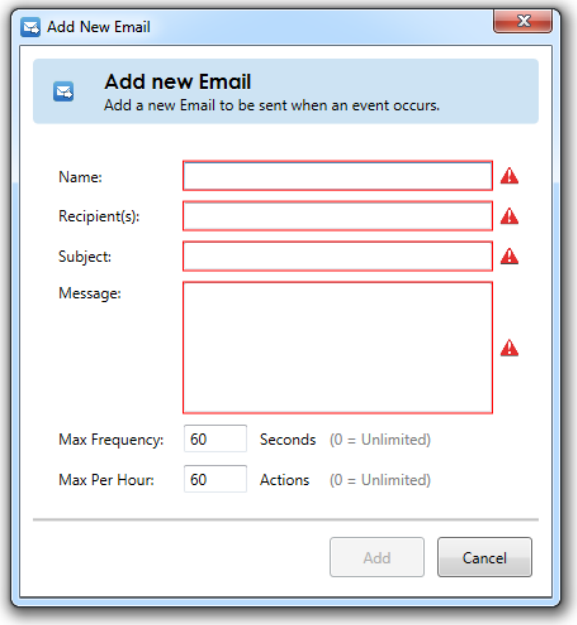


Figure 25 Configure a new email

3. Fill out the fields of the pop-up according to the following:

Item	***Description***
Name	Enter a descriptive name for the email template so that you can easily identify it.
Recipient(s)	Enter the email distribution list using standard email format (e.g. john@domain.com). If you want to send to multiple recipients, separate each with a comma.
Subject	Enter text to be used as the subject of the email.
Message	Enter text for the message body of the email.
Max Frequency	The **Max Frequency** field is set to 60 seconds as the default value. This field identifies the time interval in seconds in which you would like to monitor alerts. This feature will reduce the amount of repeated alerts within a specified timeframe. You may modify this value to any number between 1 and 3600. A zero value indicates an unlimited time period and may accumulate many unnecessary events.
Max Per Hour	The **Max Per Hour** field allows you to control the maximum number of times you want this action to be performed in an hour.

The red outlined warnings will disappear once data is entered in the correct format into each field.

4. When complete, click **Add**.

The email has been configured but has not been assigned to any particular alert. This association is done in the **Distribution Groups** tab. See *Actions* on page 129.

Once an email has been configured, you may test, edit or delete it.

To Test an Email

You can test the functionality of a configured email.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send Email** item.
3. Right-click the configured email list item and select *Test…*
4. A pop-up appears indicating that a test move will be issued.
5. Click **Send** to send a test email.
6. Click **OK** when the *Test Status* pop-up appears.

To Edit an Email

You can edit the configuration of an email if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send Email** item.
3. Right-click the configured email list item and select *Edit…*
4. Modify the changes as needed.
5. Click **Update** to save changes.

To Delete an Email

You can delete a configured email if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send Email** item.
3. Right-click the configured email list item and select *Delete…*
4. An '*Are you sure you want to delete…*" pop-up is displayed. Click **Yes** to confirm the deletion.

Send HTTP Request

Used when Ocularis is integrated with certain 3rd party systems, HTTP requests (GET and POST) can be sent when an event occurs. The requests are configured in the **Servers / Events** tab and associated with an event in the **Distribution Groups** tab.

To Configure an HTTP Request

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Right-click the 'Send HTTP Request' list item and select *Add New HTTP Request…*

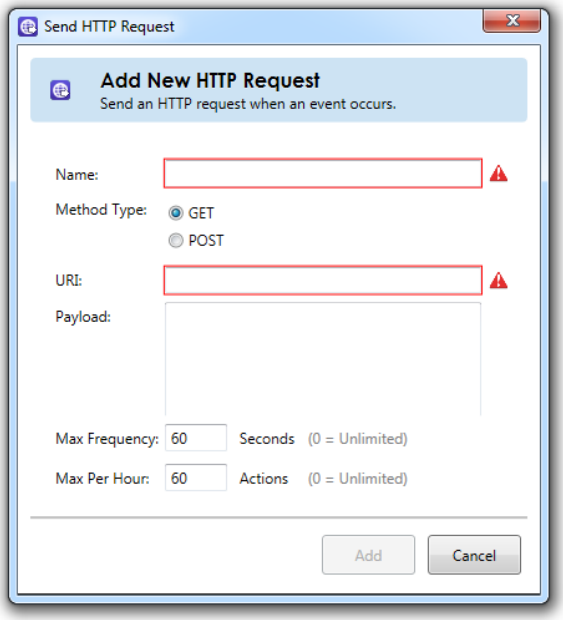


Figure 26 Add New HTTP Request

3. Fill out the fields of the pop-up according to the following:

Item	***Description***
Name	Enter a descriptive name for the request so that you can easily identify it.
Method Type	Select 'GET' or 'POST' based on your integration.
URI	Enter the URI to send the request to.
Payload	Enter the payload information to be sent.
Max Frequency	The **Max Frequency** field is set to 60 seconds as the default value. This field identifies the time interval in seconds in which you would like to monitor alerts. This feature will reduce the amount of repeated alerts within a specified timeframe. Valid values are any number between 1 and 3600. A zero value indicates an unlimited time period and may accumulate many unnecessary events.
Max Per Hour	The **Max Per Hour** field allows you to control the maximum number of times you want this action to be performed in an hour.

The red outlined warnings will disappear once data is entered in the correct format into each field.

4. When complete, click **Add**.

The HTTP Request has been configured but has not been assigned to any particular alert. This association is done in the **Distribution Groups** tab. See *Actions* on page 129.

Once an HTTP Request has been configured, you may test, edit or delete it.

To Test an HTTP Request

You can test the functionality of a configured HTTP Request.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send HTTP Request** item.
3. Right-click the configured HTTP Request list item and select *Test…*
4. A pop-up appears indicating that a test move will be issued.
5. Click **Send** to send a test HTTP Request.
6. Click **OK** when the *Test Status* pop-up appears.

To Edit an HTTP Request

You can edit the configuration of an HTTP Request if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send HTTP Request** item.
3. Right-click the configured HTTP Request list item and select *Edit…*
4. Modify the changes as needed.
5. Click **Update** to save changes.

To Delete an HTTP Request

You can delete a configured HTTP Request if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send HTTP Request** item.
3. Right-click the configured HTTP Request list item and select *Delete…*
4. An '*Are you sure you want to delete*…" pop-up is displayed. Click **Yes** to confirm the deletion.

Send TCP/UDP Data Packet

Used when Ocularis is integrated with certain 3rd party systems, data packets can be sent from Ocularis when an event occurs. The packets are configured in the **Servers / Events** tab and associated with an event in the **Distribution Groups** tab.

To Configure a TCP/UDP Data Packet

1. Expand the *Actions* node in the **Servers / Events** tab.

2. Right-click the 'Send TCP/UDP Data Packet' list item and select *Add New Data Packet…*

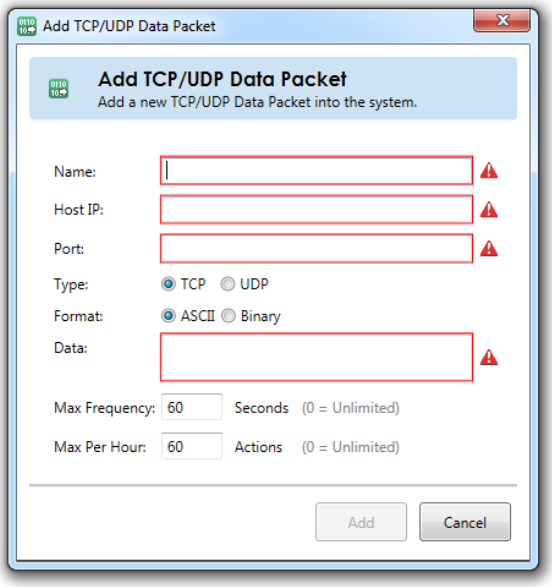


Figure 27 Add New TCP/UDP Data Packet

3. Fill out the fields of the pop-up according to the following:

Item	***Description***
Name	Enter a descriptive name for the data packet so that you can easily identify it.
Host IP	Enter the recipient host IP address.
Port	Enter the port number to use to send the data packet.
Type	Select either **TCP** or **UDP** depending on the transmission desired.
Format	Choose either **ASCII** or **Binary**.
Data	Enter the string to be sent.
Max Frequency	The **Max Frequency** field identifies the time interval in seconds in which you would like to monitor alerts. This setting will reduce the amount of repeated alerts within a specified timeframe. Valid values are any number between 1 and 3600. A zero value indicates an unlimited time period and may accumulate many unnecessary events. Default value is 60 seconds.
Max Per Hour	The **Max Per Hour** field allows you to control the maximum number of times you want this action to be performed in an hour.

The red outlined warnings will disappear once data is entered in the correct format into each field.

4. When complete, click **Add**.

The Data Packet has been configured but has not been assigned to any particular alert. This association is done in the **Distribution Groups** tab. See *Actions* on page 129.

Once a Data Packet has been configured, you may test, edit or delete it.

To Test a TCP/UDP Data Packet

You can test the functionality of a configured TCP/UDP Data Packet.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send TCP/UDP Data Packet** item.
3. Right-click the configured TCP/UDP Data Packet list item and select *Test…*
4. A pop-up appears indicating that a test move will be issued.
5. Click **Send** to send a test TCP/UDP Data Packet.
6. Click **OK** when the *Test Status* pop-up appears.

To Edit a TCP/UDP Data Packet

You can edit the configuration of a TCP/UDP Data Packet if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send TCP/UDP Data Packet** item.
3. Right-click the configured TCP/UDP Data Packet list item and select *Edit…*
4. Modify the changes as needed.
5. Click **Update** to save changes.

To Delete a TCP/UDP Data Packet

You can delete a configured TCP/UDP Data Packet if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send TCP/UDP Data Packet** item.
3. Right-click the configured TCP/UDP Data Packet list item and select *Delete…*
4. An '*Are you sure you want to delete*…" pop-up is displayed. Click **Yes** to confirm the deletion.

Events Pane

The **Event** pane of the **Servers / Events** tab is where administrators configure Ocularis events. This includes:

- Camera events are identified and video alerting is mapped between cameras and events.
- Creating associations between events and cameras.
- Creating new events, such as Data Link (Generic), Composite Events and Analytic Events.

Events configured in this tab identify system wide events. Filtering these events to individual users is configured in the Distribution Groups Tab. Ocularis events associated with cameras are supported with *Ocularis ES*, *Ocularis LS*, *Ocularis CS* and *Ocularis IS*. Generic and Composite events are supported by all Ocularis feature sets, including Ocularis PS.

> ***Note**:*
> *In order to use camera events with Ocularis Base, an event proxy related to the event (such as a recording component event proxy) must first be installed and configured to forward events to the Ocularis Base machine.*

The event proxies configured to forward camera events to Ocularis Base are listed in the **Events** pane. If the desired proxy is not shown, you should:

- Click the **Resync** button (*see Events Toolbar* on page 35).
- Double-check the event proxy installation and configuration. You may need to restart the event proxy and/or restart the *Ocularis Administrator* application in order for it to appear on this screen.

From the sample shown in Figure 28, you can see that some cameras may have more available device events than others. This is based on the camera driver itself as well as other event settings inherited from the recording component. Recorder based Generic events will also appear in this pane.

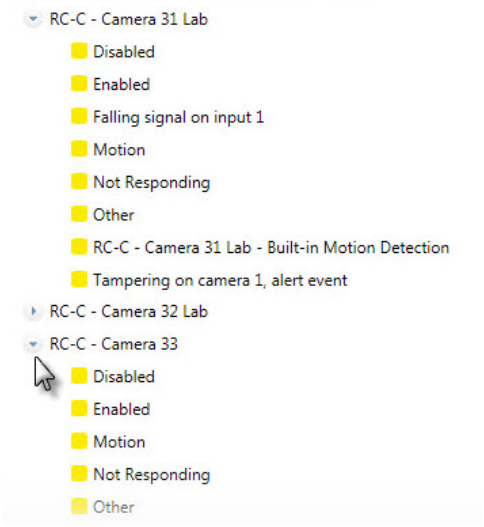
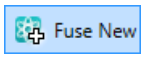
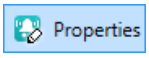
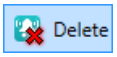
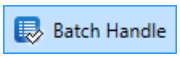
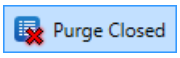


Figure 28 Expanded List of Available Events

Administrators determine which events on which camera they would like included as part of the alert notification process. This is accomplished by associating camera video with these events to create what is called an **Event Rule**.

Events Toolbar

Buttons within the *Events* pane are defined as follows:

Resync		The *Ocularis Administrator* application polls the Ocularis Base SQL database at regular intervals. If, for whatever reason, you wish to manually synchronize event data from the database with *Ocularis Administrator*, click the **Resync** button in the Events Toolbar. SQL Server data updates should now be reflected on the screen.
Fuse New		Use this to create a new composite event. See *To Configure a Composite Event*.
Properties		Use this to modify the priority or audio file of a Composite Event or Simple Event Rules.
Delete		Use this to delete Composite or Generic Events. See Data Link / Generic Events.
Batch Handle		Use the **Batch Handle Events** button to handle 'unhandled' alerts. See also: *To Batch Handle Events.*
Purge Closed		Use the **Purge Close** button to delete all closed events on the server. See also: *To Purge Closed (Handled) Events*.

Batch Handle Events

As events occur and users are alerted in the *Ocularis Client*, operators "handle" the events. (See '*Handling Alerts*' in the *Ocularis Client User Manual*.) All 'unhandled' events eventually accumulate. Administrators may remove these events and place them in a 'Closed' status by using the **Batch Handle Events** button.

To Batch Handle Events

1. In the **Servers / Events** tab, click the **Batch Handle Events** button.
   A *Batch Handle Events* pop-up appears.

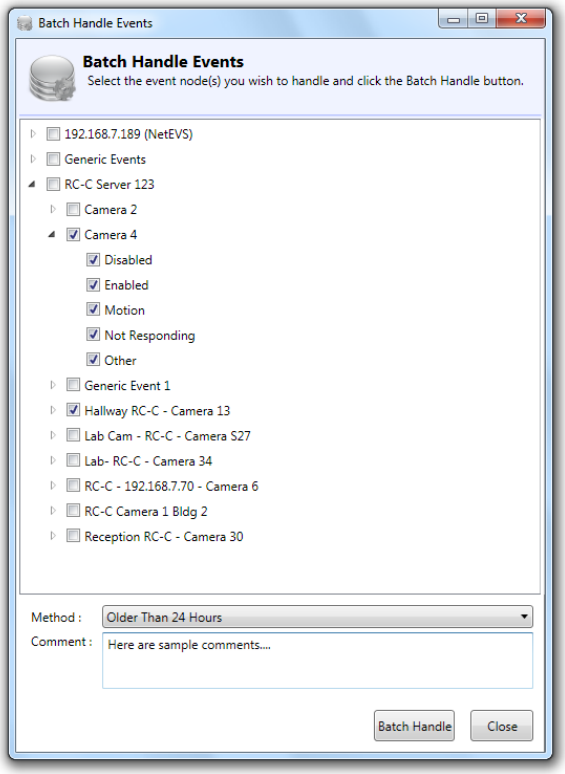


Figure 29 Batch Handle Events

2. Expand the list of events as needed and select the events for whose unhandled alerts you wish to delete. You may get as granular as you like.
3. Choose the amount of events you wish to delete in the **Method** drop-down list. The selection choices are: **Older than 24 Hours**, **Keep only last 100 events**, **Clear everything!**
4. Enter optional comments. These comments will be visible when viewing the Handled Events in the *Ocularis Client Handled Events* list.
5. Click **Batch Handle** to handle these events.

You'll be able to see these in the Handled Alerts list in the *Ocularis Client*.

Purge Closed Events

When an event is handled in the *Ocularis Client*, it becomes a handled or "closed" event. The *Ocularis Administrator* application provides a means to delete all closed events. When administrators purge closed events they are deleted permanently.

TO PURGE CLOSED (HANDLED) EVENTS

1. In the **Servers / Events** tab, click the **Purge Closed Events** button.

   An "*Are you sure you wish to delete all handled events*" warning message appears.
2. Click **Yes** to purge these events.

Simple Event Rules

Simple Event Rules identify which events will be monitored on the system. An entry to the *Ocularis Client* Alert Manager will be recorded and, if configured, video may appear in a blank screen pane. Cameras are mapped to events that are system defined (such as motion on a camera) or user defined (such as a Data Link or Composite Event).

Create a simple Event Rule by associating camera video with an event. Events which are mapped in the **Servers / Events** tab are system-wide. Administrators determine which users will get visibility to these events in the Distribution Groups Tab.

To Create an Event Rule (To Associate Camera Video with Events)

1. In the **Servers / Events** Tab, expand the **Cameras** list in the **Servers** pane for cameras you wish to associate with automated events.
2. Expand the list in the **Events** pane until you locate the event you would like to monitor.
3. For the desired event, drag & drop a camera name from the **Servers** pane to the event listed in the **Events** pane. (See Figure 30).

> ***Tip***: *If you want to associate the camera video to all events affiliated with that camera, drag & drop the camera name from the left Servers pane directly onto the camera name in the Events pane.*

When the camera video is successfully associated and an ***Event Rule*** is created, it appears in the collapsible list.

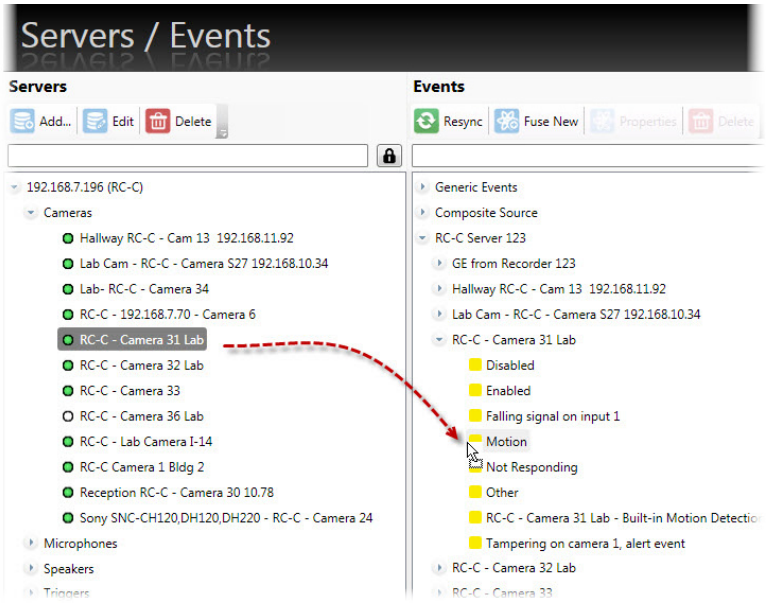


Figure 30 Drag & Drop to Associate Events

4. You may drag additional cameras to the same event for the event to have multiple camera associations.

Video generated by automated events will appear in a *Blank Screen* pane on the operator's *Ocularis Client* view. If multiple cameras are associated the an event, the cameras will appear in the blank screen as a carousel.

For the example shown in Figure 31, the events shown here are:

- If there is motion on RC-C - Camera 3, associate the camera feed from this same camera with the event.
- If RC-C - Camera 3 is not responding, register an event and associate the feed from both RC-C - Camera 2 and RC-C – Camera 1 with this event.

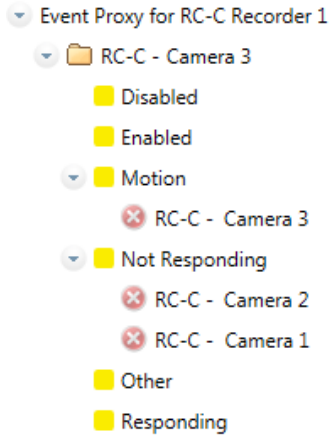


Figure 31 Associated Events

TO REMOVE A CAMERA FROM AN EVENT RULE (DISASSOCIATE A CAMERA)

1. In the **Servers / Events** Tab, expand the nodes in the **Events** pane until you see the Event Rule you wish to remove.
2. Click the next to the camera name to disassociate it from the event.

   The camera mapping is removed.

Event Properties

For the events that you wish to monitor, you may define certain parameters related to the behavior of the alert. These properties apply to simple event rules, data link/generic events or composite events. The properties are grouped into two sections:

- Alert
    - Priority
    - Audio
    - Blank Screen Only
- Retention
    - Max Events
    - Max Age
    - Max Frequency

Alert

In the Alert section, specific properties on the behavior and appears of the alert is set.

Priority

Events can be prioritized. For example: an organization may deem that the loss of video from camera 1 is critical but the loss of video of camera 7 is not. These priorities may be set by the system administrator. The priority of the event will dictate how it appears within the *Ocularis Client*.

By default, when an Event Rule is created, it is assigned a priority of 5 or *Medium*. Priority levels range from 0 – 10 where 10 is the highest priority

TO MODIFY THE PRIORITY OF AN EVENT

1. In the **Servers / Events** tab, expand the **Event Rule** in the **Events** pane whose priority you wish to change.
2. Select (highlight) the **Event** for the event rule (not the camera name).
3. Click the **Properties** button or double-click the event.
4. In the resulting **Event Rule** pop-up, select the desired priority level and click **Ok**.

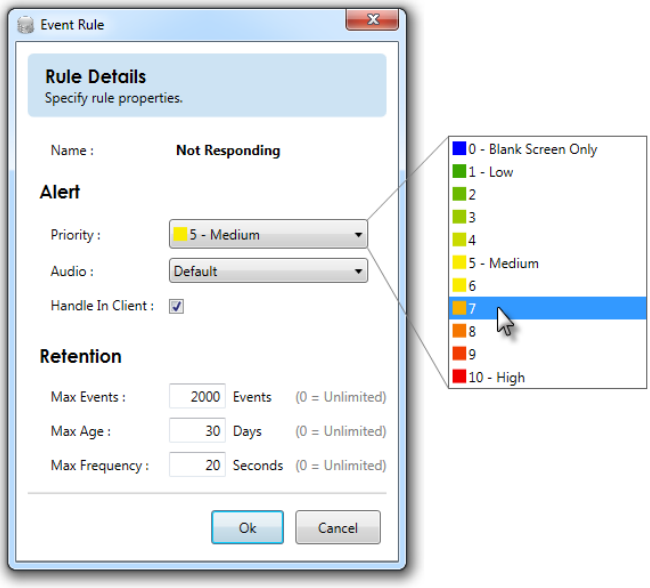


Figure 32 Event Rule Properties: Priority

Event priorities are identified in *Ocularis Administrator* and in *Ocularis Client* by color.

Priority Level	***Color Shade***	***Priority Level***
0	Blue	None
1-3	varying shades of green	Low
4-6	varying shades of yellow	Medium
7-10	varying shades of red	High

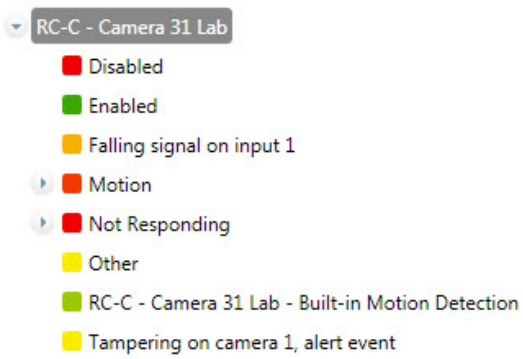


Figure 33 Priorities Color Coding sample in Ocularis Administrator

Event priorities work hand-in-hand with the *Blank Screen Only/Handle In Client* option. Priority levels determine different behavior of the alert.

Handle In Client

The 'Handle In Client' checkbox allows administrators to control which alerts they want their operators to acknowledge in Ocularis Client and which need not. In other words, if the Handle In Client checkbox is checked (or on), the alert will appear in the Alert Manager (i.e. list of unhandled alerts) when the event occurs until such time that the alert is handled (or login session has ended). The alert counter will increment for each alert. If the checkbox is not checked (or off), the alert will be shown on a Blank Screen pane (if one is displayed) and then disappear when cleared or when the dwell time is reached.

Priority 0 An alert with a Priority 0 is one where video from associated cameras will be displayed on a blank screen only. No additional data is kept or logged for these alerts. Priority 0 is used when you only want to see an event posted to a blank screen but then no longer need to monitor it. Therefore, if there is no blank screen displayed, you won't see a priority 0 event. The alert counter will not increment for alerts with this priority. By default, when you select Priority 0, the 'Handle in Client' checkbox is unchecked. This means that the event will not be logged into the database.

Priority 1-6 Alerts with Priority 1-6 are categorized low or medium. By default, these alerts will be shown on a blank screen (if one is visible) and be shown in the Alert Manager list of unhandled events until the event is handled (or the session ends). The video in the blank screen will clear after the configured dwell time for the pane in the view has been reached. If the 'Handle In Client' checkbox is unchecked, the alert will NOT appear in the Alert Manager.

Priority 7-10 Alerts with Priority 7-10 are considered high priority alerts. These alerts behave like the priority 1-6 alerts in that by default, they are to be acknowledged by operators using Ocularis Client. What makes these priority alerts different (other than their color representation), is that they remain on-screen in blank panes until acknowledged by an operator.

Audio

When an event occurs, the subsequent alert can play a sound file through the Ocularis Client as an added attention getting mechanism. The sound played can be configured by the system administrator. The same sound can be played for all alerts or configured on an alert by alert basis. A default audio setting is available. Sounds are not required and a 'no sound' option is also supported.

Audio files are imported in the **Assets** Tab where the default audio file is set. See *Event* Audio Clips on page 101 for more information on sound file configuration.

TO MODIFY THE AUDIO OF AN EVENT

1. In the **Servers / Events** tab, expand the **Event Rule** in the **Events** pane whose sound you wish to change.
2. Select (highlight) the **Event** for the event rule (not the camera name).
3. Click the **Properties** button or right-click the event and select **Properties**.
4. In the resulting **Event Rule** pop-up, from the Audio drop-down, select the desired sound file, **None** or **Default**.
    - If you click 'None', no sound file will be played when the event occurs. If there is no option available labeled 'None', then 'None' must already be set as the default option. Select 'Default'.
    - If you select a .wav file, that sound will play through the Ocularis Client when the event occurs.
    - If you select 'Default', you may get a sound file or no sound, depending on the default setting in the **Assets** tab. In the event where 'None' is configured as the default audio in the **Assets** Tab, the option 'None' will not be visible in the drop-down list. In this case, selecting 'Default' is equivalent to

selecting 'None'. You should be aware of the default audio setting in the **Assets** Tab when configuring events.

5. Click **Ok**.

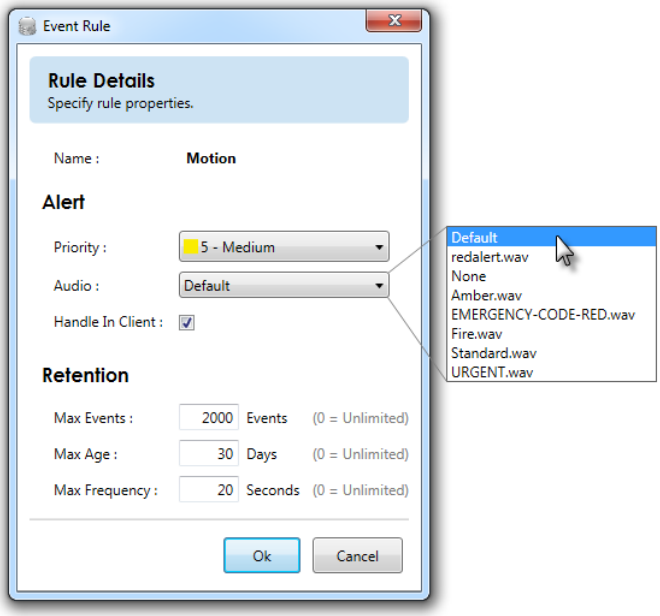


Figure 34 Event Rule Properties: Audio Samples

Event Retention

Depending on the environment, the types and number of events monitored, the amount of events can quickly build up in the system. The database can be overcome with too many events. The operator's blank screen panes may also be cluttered by repetitive or too many events. Therefore, system administrators have the ability to limit the events that are stored and retained in the database and shown on a blank screen. These parameters are found when configuring an event rule (basic, generic or composite).

Max Events

This field holds the total count of event instances to save to the database for the event rule. For instance: if this value is set to 10 for a motion event on Camera A, then only 10 motion events for Camera A will be in the database at any given time. Once 10 events have accumulated and new events occur, the oldest event will be deleted and the newer event will be stored. Valid values are between 0 (the default which means unlimited) and 2,147,483,647. The default setting is 2000. Keep in mind that this field works in conjunction with 'Max Age' and 'Max Frequency'.

Max Age

The 'Max Age' for an event rule is the number of days (in 24 hour multiples) in which to store events generated by the event rule. The time is calculated from when the event took place. For instance: if this value is set to 7 for a motion event on Camera A, then each of Camera A's motion events will be deleted ('expire') 7 days or 168 hours after they

take place. The value is measured in days between 0 (unlimited and the default value) and 2,000. The default setting is 30 days. Keep in mind that this field works in conjunction with 'Max Age and Max Events'.

Max Frequency

This field identifies the time interval in seconds in which you would like to monitor alerts. This feature will reduce the amount of repeated alerts within a specified timeframe.

For instance, if the Max Frequency is set to 10 (seconds) for a motion event on Camera A and then motion occurs:

1. the timer is theoretically set to zero and the clocks starts. The event is registered in the Alert Manager and sent to the Operator's blank screen pane.
2. If the same motion event on camera A occurs again in the next second, nothing will happen.
3. If the same motion event on camera A occurs again in the second after that, nothing will happen.
4. If the same motion event on camera A occurs again for the next 8 seconds, nothing will happen.
5. At the 11th second, if the motion event on Camera A occurs, register the event in the Alert Manager, display it on the Operator's blank screen pane and reset the timer to zero.

The value is measured in seconds between 0 (unlimited and the default) and 3600 (one hour). The default setting is 20 seconds. Keep in mind that this field works in conjunction with 'Max Events' and 'Max Age'.

Event Properties Combined

Keep in mind that three event properties work in combination with each other. The 'Max Events', 'Max Age' and 'Max Frequency' all affect the amount of events that are stored and the duration of their storage.

Composite Events

A *Composite Event* (also called 'Event Fusion") is combination of two other events defined with a specific relationship and timeframe. The following are examples of a composite event:

If there is motion on Camera 1 and within the next 5 seconds there is motion on Camera 2, register an event

or

If there is a card swipe detected from an access control panel AND there is an analytic event that determines two people entered ("tail-gating"), trigger an alert

Composite Events are supported by all feature sets of Ocularis.

TO CONFIGURE A COMPOSITE EVENT

1. In the **Servers / Events** tab, click the **Fuse New Event** button.
2. Fill out the **Composite Event Rule** pop-up.

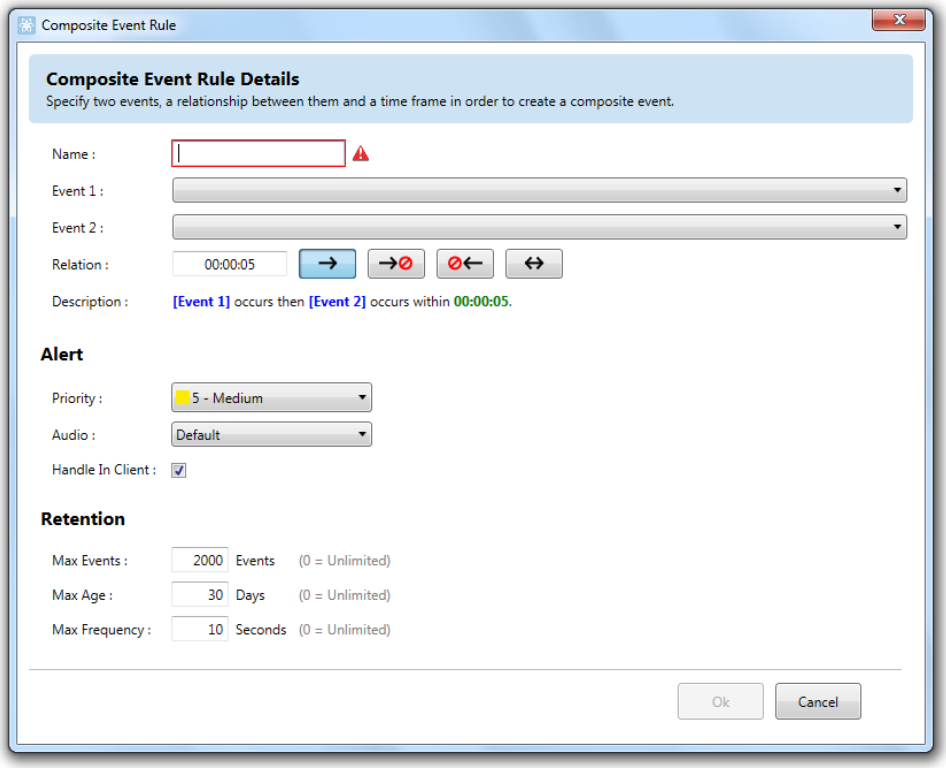


Figure 35 Configure a Composite Event: Rule Details Tab

Fields are defined as follows:

Item	***Description***
Name	Enter a descriptive name for the composite event. Avoid using special characters for the event name.
Event 1	Select an event to begin to define the condition for which the rule alert should be met. This event may be an Event Rule, Generic Event, another composite event or any event listed.

Item	Description
Event 2	Select a second event to finalize the condition for the composite formula. This event may be an Event Rule, Generic Event or another Composite Event.
Relationship	You must indicate how event 1 is related to event 2. The directional arrows define the relationship between two Event Rules and are defined below. In addition, a time period must be specified. This works in conjunction with the relationship icons in identify a time limit that may apply to the relationship. Valid times are: HH = 0 through 23 MM = 0 through 59 SS = 0 through 59
Description	As you build your composite event, a description appears in this section helping you understand rule's meaning.
Priority	Select a Priority for the composite event. See *Alert* In the Alert section, specific properties on the behavior and appears of the alert is set. Priority on page 39 for more information about priorities.
Audio	Select the sound file to be played when the composite event occurs. See *Audio* on page 41 for more information about audio.
Handle In Client	If this checkbox is checked (on), Ocularis Client will receive a registry entry for the event and (depending on priority) may require the operator to manually acknowledge the alert. See *Handle In Client* on page 40 for more information.
Max Events	Set the maximum number of event registries to retain for this composite event. See *Event Properties* on page 39 for more information.
Max Age	Set the maximum age to save event registries for this event. See *Event Properties* on page 39 for more information.
Max Frequency	Set the frequency for this event. See *Event Properties* on page 39 for more information.

Relationship Icons

	If Event 1 occurs **before** Event 2 occurs
	If Event 1 occurs but Event 2 does not occur within the specified time period
	If Event 1 does not occur in the time period defined, prior to Event 2 occurring.
	If Event 1 and Event 2 occur within the time period specified.

Please note:

- You may effectively nest composite events with other composite events resulting in a highly complex fusion of events. Consider, however, that the more complex an event, the more difficult troubleshoot may become.

- If you do not see a recently created generic event in the list of available events in the Event1 or Event2 drop-down list, click the **Resync** button to refresh the Events pane.

Refer to the example shown in Figure 36: This composite event will trigger an alert if there is an Access Denied code registered from the main door access system and 20 seconds later there is motion on the hallway camera (indicating that someone has gained illegal access).

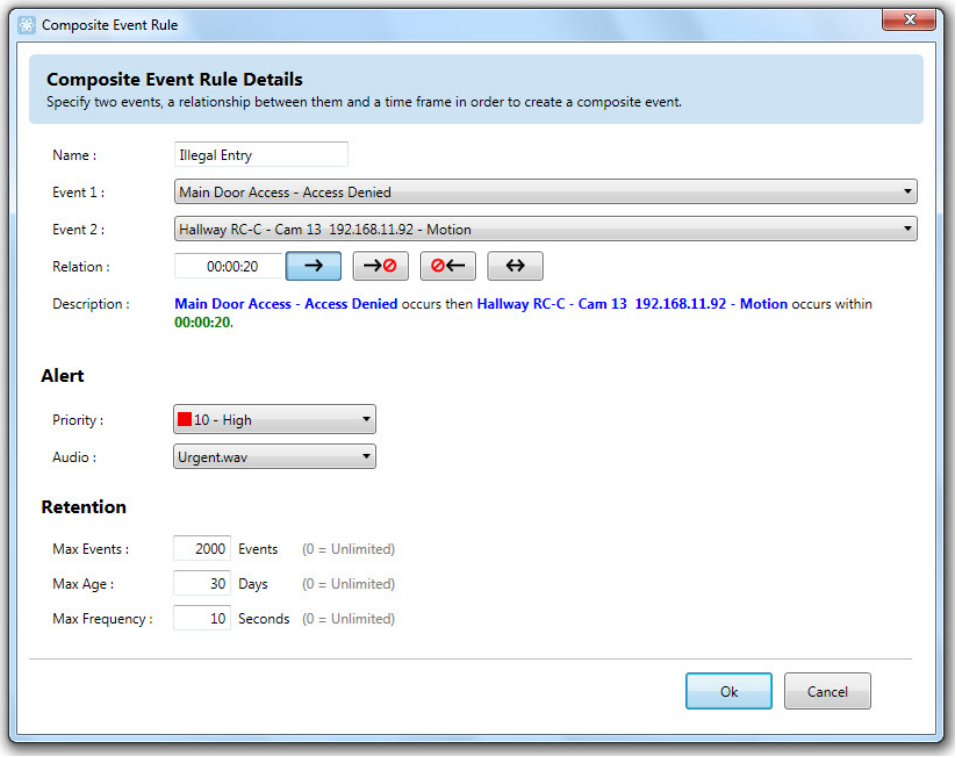


Figure 36 Composite Rule Example

TO MODIFY A COMPOSITE EVENT

1. In the **Servers / Events** tab, locate the Composite Event in the **Events** pane under the Composite Source node.
2. Highlight the Composite Event.
3. Click the **Properties** button.
4. In the resulting *Edit Composite Event* pop-up, modify desired settings.
5. Click **Apply** to save changes.

TO DELETE A COMPOSITE EVENT

1. In the **Servers / Events** tab, locate the Composite Event in the **Events** pane under the Composite Source node.
2. Highlight the Composite Event.
3. Click the **Delete** button.

4. You will be prompted with the message:

   "Are you sure that you want to delete this composite event rule?"
5. Click **Yes** to delete the Composite Event.

Data Link / Generic Events

Ocularis Base has the ability to analyze TCP or UDP data packets and automatically trigger an alert when specified criteria are met. This expands event coverage to external devices such as access controls systems. These events are called *Data Link* or *Generic* events. Generic events may be used in Blank Screen monitoring and they are supported by all feature sets of Ocularis.

Components of a Data Link / Generic Event

Data Link / Generic Events are made up of *Connections* and *Rules*. Connections define the protocol and port which Ocularis should monitor and analyze for the event. This is considered the *event source*. Rules allow you to define the actual string that should be used in the analysis of the event source. You may have multiple rules defined for the same connection and these rules may also be used in Composite Events.

TO CREATE A DATA LINK / GENERIC EVENT

Creating a Data Link / Generic Event involves these steps:

- Create a Connection to define the event source.
- Define at least one rule for the Connection.
- Test the Rule
- Map camera video to the rule to enable it and allow for Blank Screen monitoring.

TO CREATE A CONNECTION FOR A DATA LINK / GENERIC EVENT

1. In the **Servers / Events** tab, expand the *Generic Events* node in the **Events** pane.
2. Click **[add connection..]**

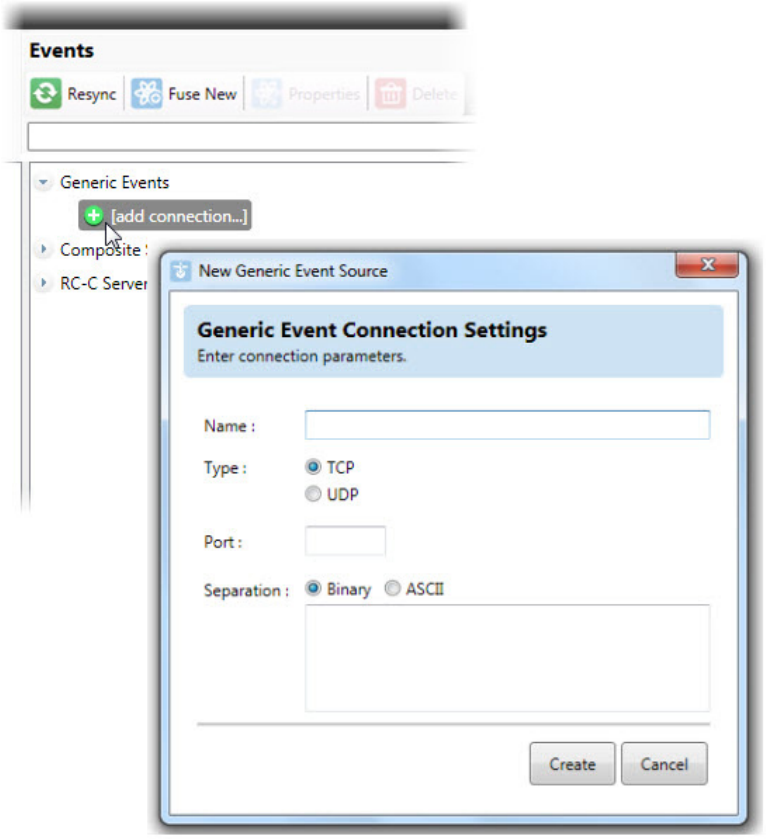


Figure 37 Add a Generic Event Connection

3. Fill out the fields in the resulting *New Generic Event Source* pop-up window as defined below. You may need to contact or review the manufacturer specifications of the device for which you are configuring the event.

Item	***Description***
Name	Enter a descriptive name for the Event Source. This is what will appear in the alert so be as descriptive yet concise as possible. Avoid using special characters in this name. For example: *Front Entrance* might be used to describe alerts transmitted access control systems on the main door to the facility.
Type	Select the protocol (**TCP** or **UDP**) based on the device you are monitoring.
Port	Enter the port on which Ocularis Base should listen for the data sent by the event source.
Separation	Select the format for data transmission. (**Binary** or **ASCII**) You may also enter a Separation character to identify to Ocularis Base, when an end of string as been received. Enter this character in the Separation field.

4. When pop-up is complete, click the **Create** button.

The Connection for the event source should be listed under *Generic Events* in the **Events** pane.

To Define a Rule for a Data Link / Generic Event Connection

Be sure to first define an event source prior to defining a rule. See *To Create a Connection for a Data Link / Generic Event* on page 47.

1. In the **Servers / Events** tab, expand the Generic Events node in the **Events** pane and select the desired generic event.
2. Expand the generic event connection source.

Figure 38 Click [add rule…] to configure the generic event connection

3. Click **[add rule..]** beneath the event.

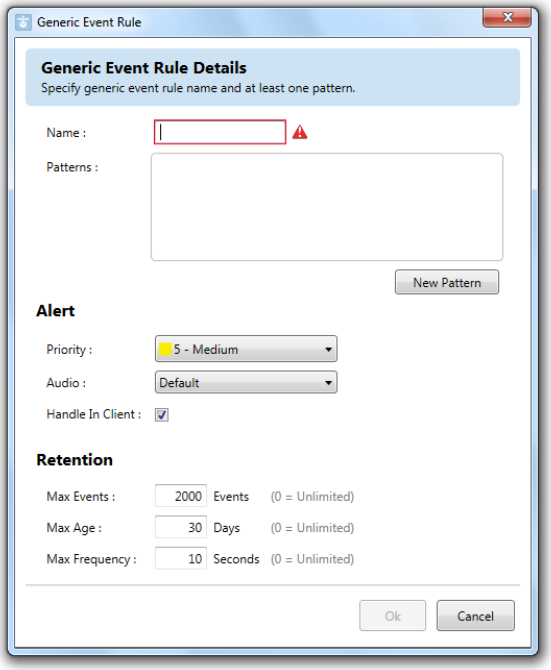


Figure 39 Creating a Generic Event Rule

4. In the resulting pop-up window, fill out the fields as follows:

Item	***Description***
Name	Enter a descriptive name for the rule. Avoid using special characters in the name field. Following our earlier example, the name could potentially be something like: *Access Denied* or *Access Granted*.
Patterns	Click the **New Pattern** button to open up a row for pattern definition. See Patterns for Rules below for more information.

Item	Description
Priority	Assign a priority for the rule. See *Event Properties* on page 39 for more information on event priorities.
Audio	Select an sound file to play when the event occurs. This selection is optional. See *Event Properties* on page 39 for more information on event audio.
Handle In Client	If this checkbox is checked (on), Ocularis Client will receive a registry entry for the event and (depending on priority) may require the operator to manually acknowledge the alert. See *Handle In Client* on page 40 for more information.
Max Events ***Max Age*** ***Max Frequency***	Set the retention parameters for this event. See *Event Properties* on page 39 for more information on event retention.

5. Click **OK** when done.

You may define multiple rules for the same generic event connection.

Patterns for Rules

When specifying the logic for Ocularis Base to use when analyzing data packets you have several options. You must know the string or a portion thereof that you wish to look for in order to trigger the event. The options for searching for the string are as follows:

Item	Description
Matches	The string you specify must be detected in its entirety with exactly the characters you specify.
Contains	The string you specify can be located anywhere within the string of the data packet.
Starts With	The data packet must begin with the string you specify.
Ends With	The data packet must end with the string specified.

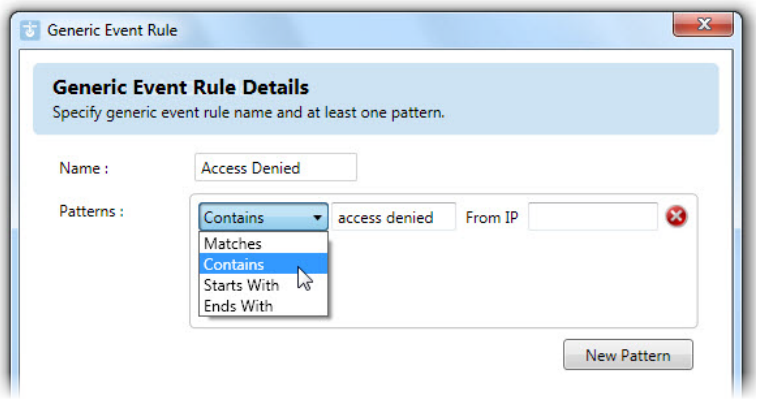


Figure 40 Patters for Generic Events

Sources for Patterns

For each string to be analyzed on a specified port, you can also limit the analysis to be from a specific IP address. For TCP based connections, enter the IP address for the pattern for which you wish to restrict analysis in the **From IP** field. This is an optional field. If left blank, the pattern will be evaluated on any IP address.

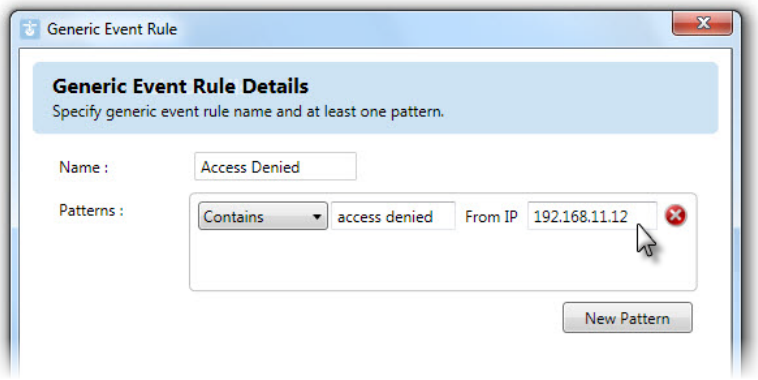


Figure 41 Specify source IP of Pattern

You may include multiple patterns for the same rule. The Boolean logical operator “OR” will be applied for each.

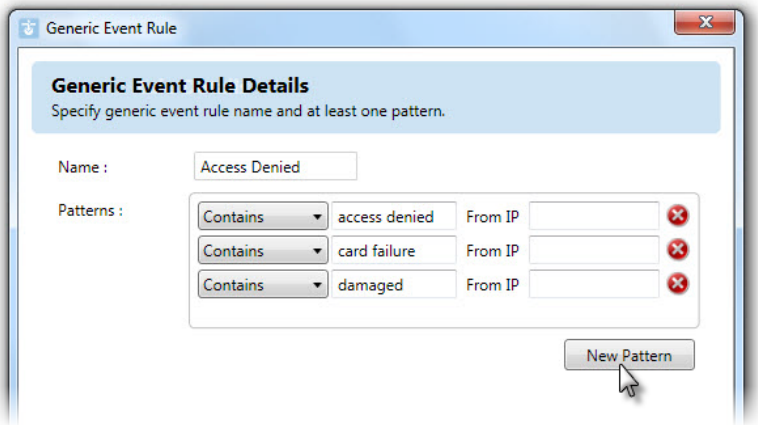


Figure 42 Using Multiple Patterns

Click the **New Pattern** button to add a row to configure each pattern.

In the example shown in Figure 42, the following generic event is configured: “if the text string ‘access denied’ or ‘card failure’ or ‘damaged’ appears within the specific port of the connection, trigger the *Access Denied* Rule. (the port is configured with the connection).

TO MAP THE RULE

Once the rule has been created, you may associate video from a camera to this event. Do this by dragging and dropping the camera from the *Servers* pane to the Generic Event on the *Events* pane. Follow the same steps as discussed in *To Create an Event Rule (To Associate Camera Video with Events)* on page 37.

DETERMINE ALERT DISTRIBUTION

Configuring alerts for events does not automatically activate them. Additional steps are needed to assign who should receive notification for which alert and when. Administrators determine which users will get notification of associated events in the Distribution Groups Tab. This step needs to occur in order to see alert video, to transfer alerts from Ocularis Base to Ocularis Client operators or to test a Generic event.

TO TEST THE DATA LINK / GENERIC EVENT

You can perform a manual test of the Data Link/Generic event to determine if it is properly configured.

1. In the **Servers / Events** tab, expand the Generic Events node in the **Events** pane to expand it and select the Generic Event.
2. Expand the Connection by clicking the expand symbol next to it.
3. Click the lightning bolt symbol adjacent to the rule name.

   A *Generic event rule tester* pop-up appears.

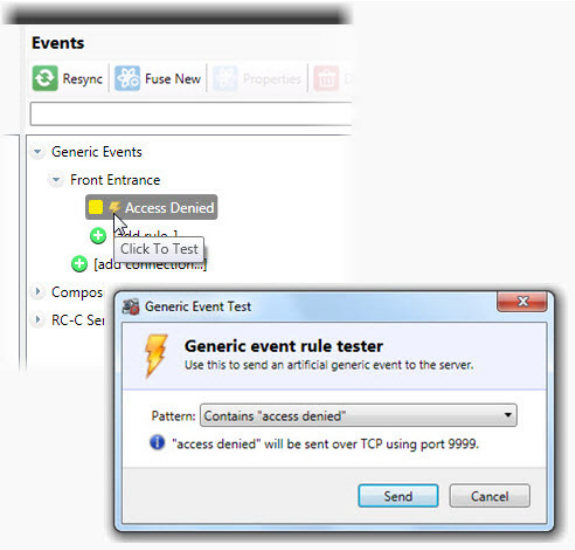


Figure 43 Testing Generic Events

4. You can select any pattern associated with the event from the drop-down list to test.

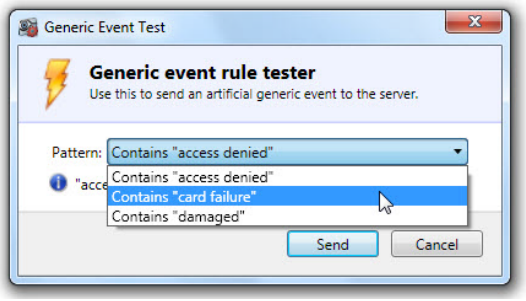


Figure 44 Selecting a Pattern to Test

5. Click **Send**.

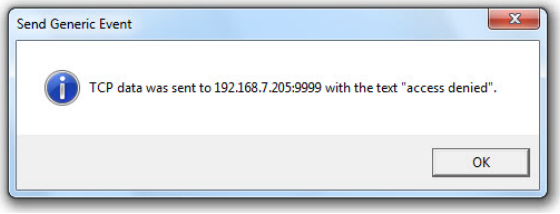


Figure 45 Generic event test data sent confirmation

A test event will be generated and sent based on configured rules.

Device Filter / Event Filter

As the system grows and more and more cameras and devices are added, it can take some time to locate the desired device amongst the list of hundreds or even thousands of devices. The same applies to events. If there are dozens or hundreds of events, it can be cumbersome to try to locate a specific event. To alleviate this, a 'Device Filter' and 'Event Filter' are available from the **Servers / Events** Tab.

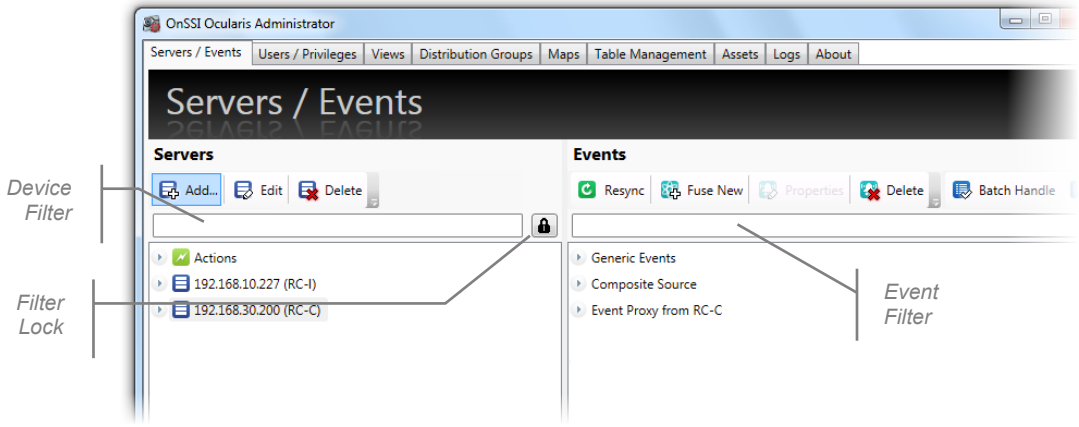


Figure 46 Device and Event Filters

To Use the Device Filter

1. From the **Servers / Events** tab, type a portion of a string to filter the device list in the 'Device Filter' text box. The string can contain letters, numbers or special characters. The filter is not case sensitive. The resulting list will be an exact match of the content typed into the Device Filter text box.

   For instance, in Figure 47, the filter is for all 'lab' devices.

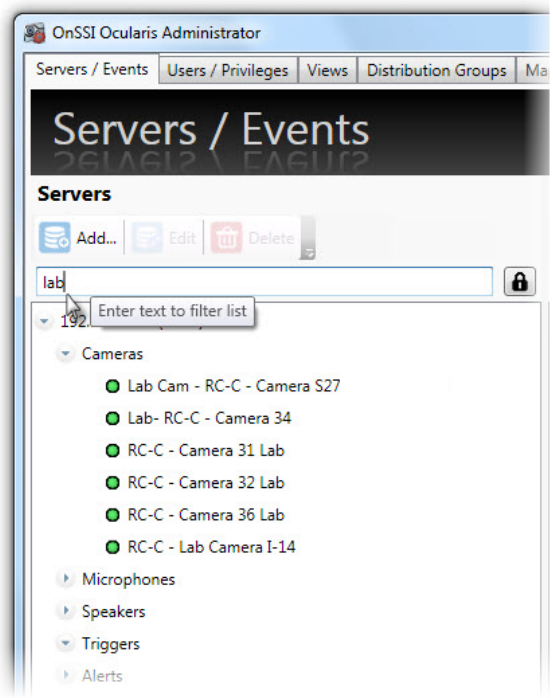


Figure 47 Filter for 'lab'

You may clear the filter by deleting the text in the Device Filter text box.

TO USE THE EVENT FILTER

1. From the **Servers / Events** tab, type a portion of a string (or keyword) to filter the event list in the 'Event Filter' text box. The filter is not case sensitive.

   The list will display only those events whose name includes the text typed. For instance, in Figure 48, the filter is for all events related to 'fire'.

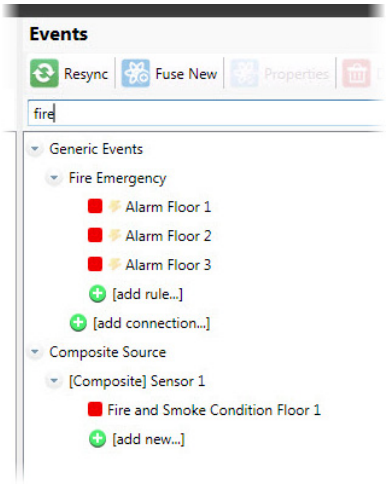


Figure 48 Event Filter for 'fire'

Filter Lock

You may use the 'Filter Lock' icon to lock the filter. This will disable the 'Event Filter' text box from accepting entries and allow the 'Device Filter' to filter both devices and events. This makes locating events related to a particular device quick and easy.

TO USE THE FILTER LOCK

1. From the **Servers / Events** tab, first type a portion of a string to filter the device list in the 'Device Filter' text box. The filter is not case sensitive.
2. Click the 'Filter Lock' icon.

   The filter text from the 'Servers' list is now applied to the filter of the 'Events' list. The filter will apply to both panes.

   For instance, the sample shown in Figure 49 shows the Device Filter and Event Filter for all 'Lab' cameras and associated events.

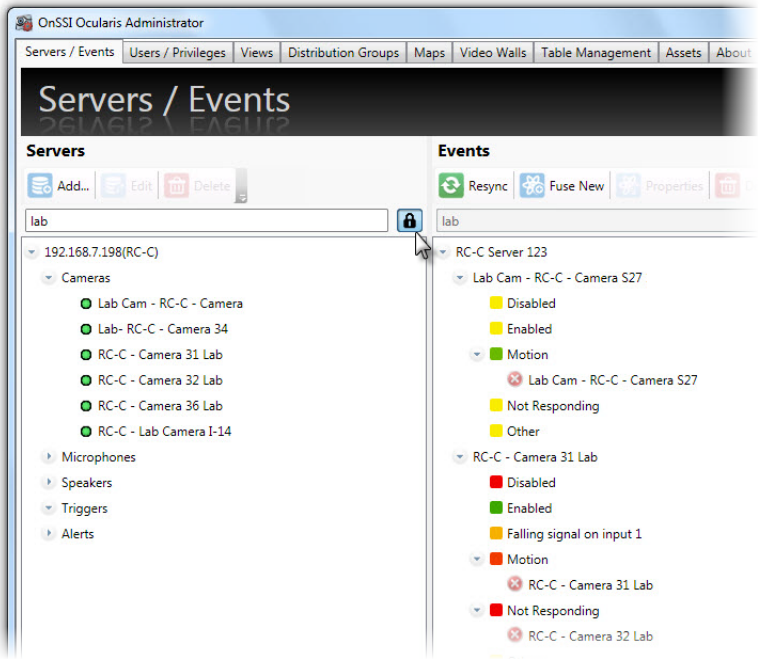


Figure 49 Filter for 'Lab' cameras and events

Users / Privileges Tab

This tab is used to define users, user groups and camera privileges within an Ocularis system.

The Ocularis User Group/User Hierarchy

Access to the Ocularis surveillance environment is controlled through the use of **User Groups** and **User Accounts**. User Groups are assigned access and privileges to various components of the system. An example would be to assign a specific set of cameras or video wall to a user group. Once a group's operating parameters are established, user accounts can simply be assigned to the group and inherit the privileges of the group. Furthermore, each user account within a group may have alternative privileges set beyond those of the group.

Privileges to cameras may be controlled through *camera privilege groups*. These groups allow you to organize a set of cameras *per user group* and apply specific parameter restrictions to the camera group as a whole.

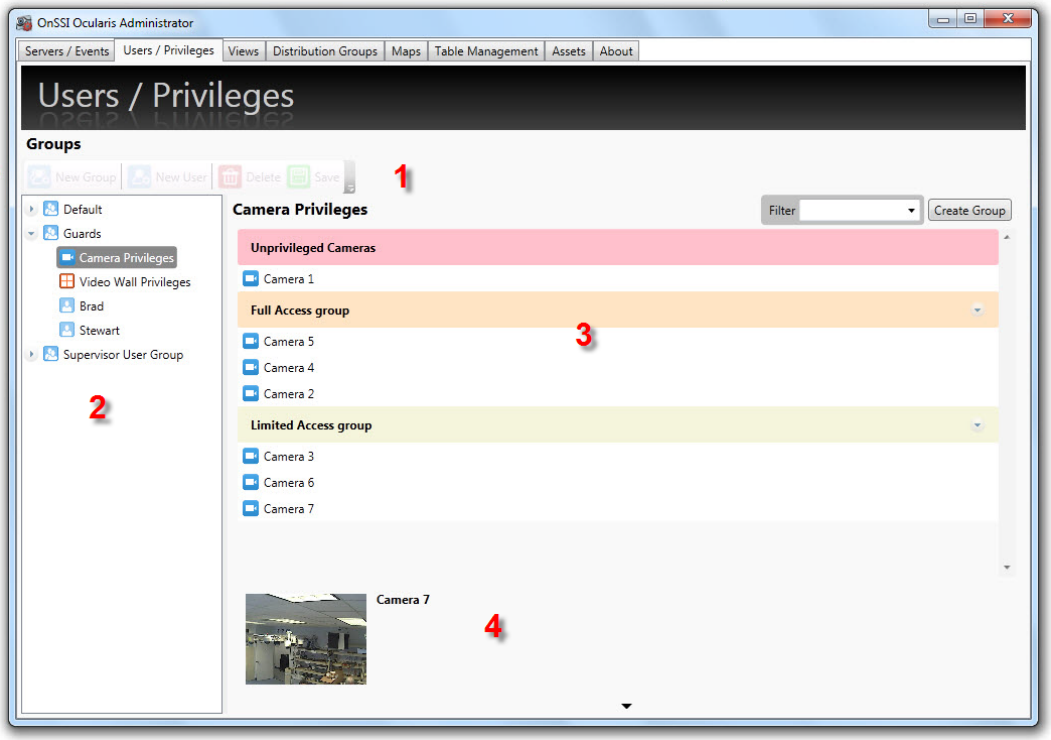


Figure 50 Users / Privileges Tab

The **Users / Privileges** Tab is divided into several sections:

1. Near the top, there is a toolbar containing several function buttons that apply to items on the tab.
2. On the left, there is a **Groups** pane that displays existing groups and users and their hierarchy.
3. On the right, the pane will display details for the item selected in the Groups pane.
4. For cameras only, a preview pane is available displaying the camera's thumbnail image.

User / Privileges Toolbar

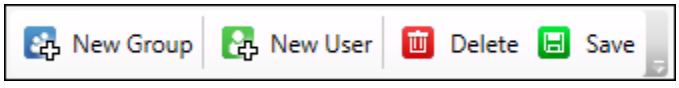


Figure 51 Users / Privileges Toolbar

Working with User Groups

The installation process creates one user group titled **Default**. This user group has two user accounts: **Admin** and **Guest** (each has a matching password).

The 'Admin' user account is an administrative user account. The Admin user can view and change anything in *Ocularis Administrator*. We recommend changing the password of this account immediately. This account is referred to as a *super user* account.

The 'Guest' account is what can be considered a *standard* account. This means that, by default, this user can access video through the *Ocularis Client* but will not be able to log in to the *Ocularis Administrator*.

Neither the 'Admin' nor the 'Guest' account may be deleted.

TO CREATE A USER GROUP

1. In the **Users / Privileges** toolbar, click the **New Group** button.
2. An entry in the list called **New Group** appears. Edit the text to the group label you wish to create.
3. Press **[ENTER]**.

The new group appears in the list. Repeat this process for each group you wish to add.

TO MODIFY A USER GROUP NAME

1. In the **Users / Privileges** Tab, double-click group name in the **Groups** list.
2. Edit the text to the group label as needed.
3. Press **[ENTER]**.

The updated group name appears in the list.

TO DELETE A USER GROUP

1. In the **Users / Privileges** Tab, select the group you wish to delete.
2. Click the **Delete** button on the toolbar.

   An "*Are you sure you want to delete this group*…?" warning message appears.
3. Click **Yes** to delete the group.

User Group Privileges

Privileges to specific functions of Ocularis may be set on a user group basis. Then, any user that is added to the user group may inherit the privileges set at the user group level. Default settings for most privileges is *Allowed*.

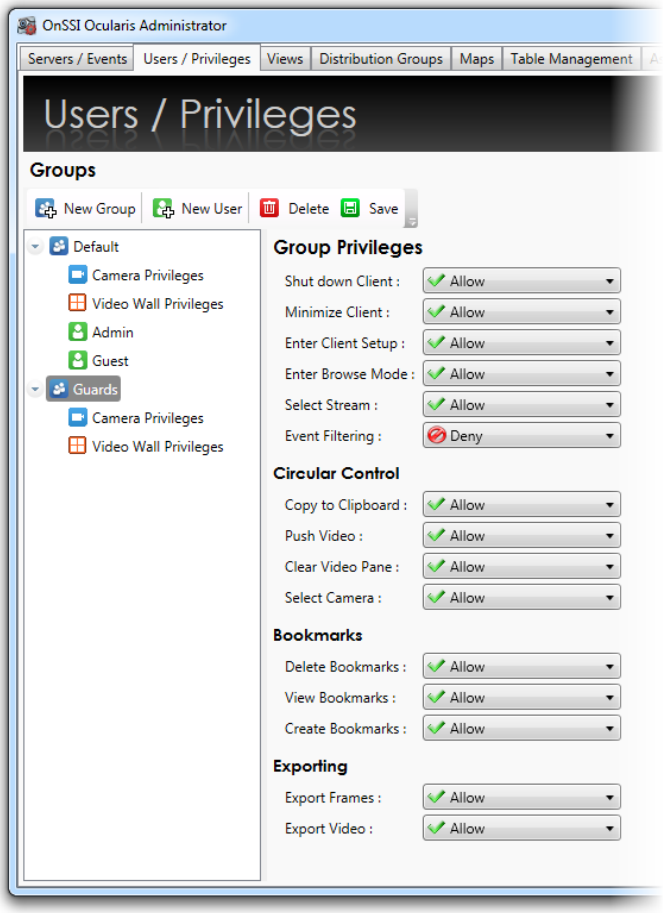


Figure 52 User Group Privileges

Users within a user group may further have alternate privileges set on a user level

Group Privileges Defined

Item	*Privilege*
Group Privileges	
Shut down Client	The user may exit Ocularis Client. When this option is 'Denied', the user must enter account credentials for an account who may log off or shut down the client application.
Minimize Client	The user may minimize the Ocularis Client application.
Enter Client Setup	The user may launch and make personal changes to Ocularis Client settings.
Enter Browse Mode	The user may leave Live mode and view recorded video.
Select Stream	The user may select between multiple live streams for a supported camera.
Event Filtering	The user may configure schedules for the automatic handling of

Item	*Privilege*
	events. This privilege is set to 'Deny' by default as it should only be allowed for limited users.
Circular Control	
For each item in this section, the 'Allow' privilege will display the corresponding function on the Circular Control menu in the *Ocularis Client*.	
Copy to Clipboard	The user may copy the displayed image to the Window's clipboard. The clipboard image may be pasted into any compatible application.
Push Video	The user may send video to another user logged in to Ocularis Base.
Clear Video Pane	The user may remove the video stream from the current pane.
Select Camera	The user may select another privileges camera from the current pane.
Bookmarks	
Delete Bookmarks	The user may delete any bookmark to which they have access.
View Bookmarks	The user may view bookmarks that they or other members of their group create.
Create Bookmarks	The user may export bookmarks from Browse mode of the *Ocularis Client*. This will only be applicable if the value in *Browsing Limit* on the camera is not equal to 0.
Exporting	
Export Frames	The user may export still images in .jpg format from Browse mode of the *Ocularis Client*. This will only be applicable if the value in *Browsing Limit* on the camera is not equal to 0. This privilege also controls whether the user may take a snapshot of video in Ocularis Client (live or browse mode).
Export Video	The user may export video in both .AVI and Database Format from Browse mode of the *Ocularis Client*. This will only be applicable if the value in *Browsing Limit* on the camera is not equal to 0.

To Modify a Group Privileges

1. In the **Users / Privileges** tab, select the User Group that you wish to modify.
2. From the drop-down menu next to the corresponding privileges, select the privilege to assign to the user group.

Figure 53 Modify a User Group Privilege

3. Click **Save**.

User Privileges

Once privileges have been established for user groups, Ocularis users need to be created and assigned to the groups.

There are three user roles in Ocularis Base: **Administrator**, **Group Administrator** and **Standard**.

User Role	*Description*
Standard	This user can access video from recorders using the *Ocularis Client* by logging into Ocularis Base. This user has no access to *Ocularis Administrator*.
Group Administrator	This user has limited access to *Ocularis Administrator*. He or she can log into *Ocularis Administrator* but may only manage their own user group or its settings. This user can add, modify or delete users in their own user group as well as modify other aspects of *Ocularis Administrator* as it applies to this user group. This user may not add, edit or delete servers. Additionally, there are some restrictions placed on Distribution Groups which will be discussed in Distribution Groups Tab on page 125.
Administrator	This is the super user for Ocularis Base. It is the user account **admin**. This user may view, change or edit any part of the system. We recommend changing the password for this account.

To Create a User Account

1. In the **Users / Privileges** Tab, select the user group to wish you would like to add users.
2. Click the **New User** button.
3. In the **Add User** pop-up window, enter the **User name** to be created.
   - User names are not case sensitive
   - User names must begin with a letter (a through z)
   - User names may not contain the following characters: **[ ] * ? @ < > / = + | \ " : , ;**
   - The **** character is allowed only when specifying the domain along with the user name such as: **onssi\jsmith**

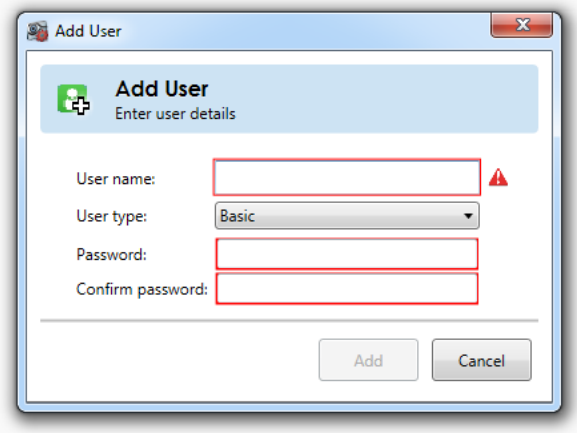


Figure 54 Add New User

As valid values are entered into each field, the red warning box will disappear.

4. Select the **User type**:

Type	***Description***
Basic	Select **Basic** if not using Windows Active Directory
Windows User	Select **Windows User** if logging in with the local Window's user account
Windows Group	Select **Windows Group** if user is to log in via Windows Active Directory Group

> ***Note**:* If the Windows User you are creating is part of a domain, you must include the domain when you enter the User Name. Use the format: **domain\username** in the User Name field

> ***Note**:* When adding a Windows Active Directory user to Ocularis Base, the system administrator can bypass the validation check for this user account if the username cannot be found by the system. This provides configuration flexibility for environments where the Ocularis Administrator is unable to check the validity of a user.

5. Enter a **Password** for this user.

   A password:

   - Is required
   - Must contain at least 4 characters
   - May contain letters, numbers, special characters and spaces
   - Is case sensitive
   - Does not expire

6. Re-enter the password to ensure accuracy.

7. Click **Add**.

8. Repeat for all users.

The user account will inherit all privileges of the group in which it is placed.

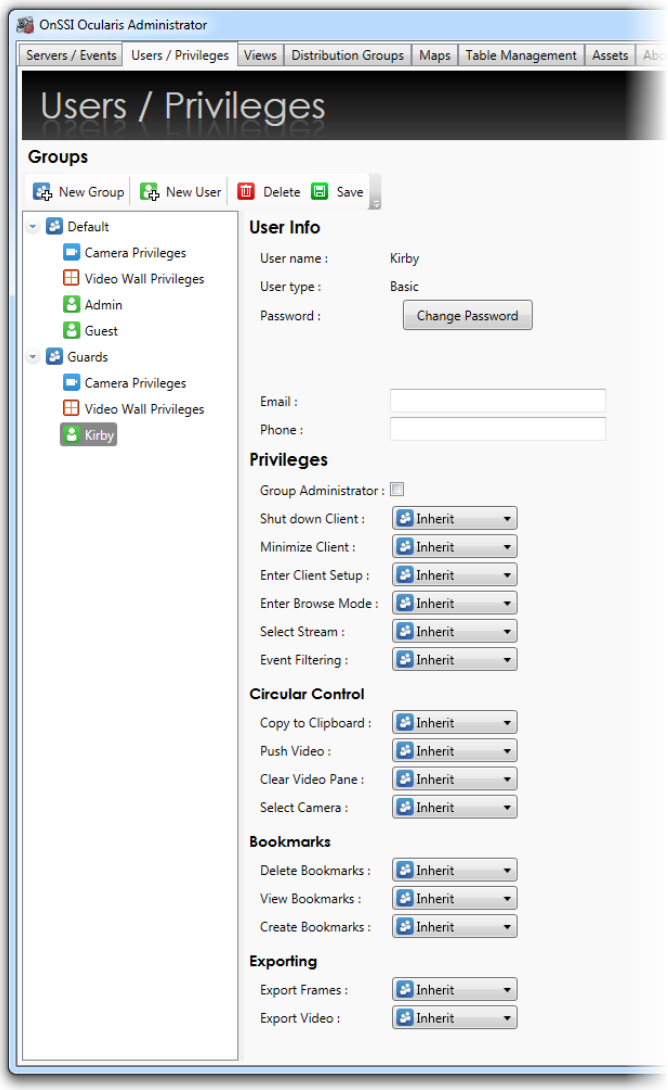


Figure 55 New User Account

TO MODIFY USER ACCOUNT SETTINGS

Administrators may reset the password or modify privileges for a user account. Group Administrators may perform these actions only for those users in his/her own group. User accounts may have differing privileges (additional or fewer) than the group to which it belongs.

1. In the **Users / Privileges** Tab, select the user account you wish to modify.
2. In the details pane you can:
    a. Change the user account password
    b. Add or edit the user's contact information (email address or phone number).
    c. Set or remove Group Administrator privilege on the user account.

d. Modify the specific user account privilege as needed. By default, new users are set to 'Inherit' privileges from the user group's setting.

***To modify a specific user account setting*:**

i. Select the drop-down list next to the corresponding privilege.

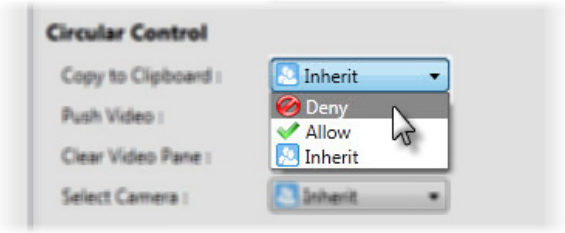


Figure 56 Modify User Privilege

ii. Change the setting: **Allow** or **Deny**

iii. Repeat for other privileges

3. When finished modifying user account settings, click the **Save** button.

If the User name or User type needs to be changed, you should delete the user account and recreate it with the proper settings.

TO DELETE A USER ACCOUNT

1. In the **Users / Privileges** Tab, select the user account you wish to delete.
2. Click the **Delete** button.

   An "*Are you sure you want to delete this user*…?" warning message appears.
3. Click **Yes** to delete the user account.

Device Privileges

Ocularis provides administrators centralized control for assigning privileges to users for all cameras on the system regardless of the recorder on which it resides. Users will not be able to view camera video unless they are given access privileges in the **Users / Privileges** tab of the *Ocularis Administrator* application. Access to a device is granted at the group level and individual functions for that device may also be granted or denied.

> ***Note**: Be sure to set privileges for the **Default** group. This includes the user **admin**. The Default group should typically be given access to all devices.*

Assign Devices To A User Group

There are three general steps in providing user groups access to devices:

- Create a Camera Privilege Group
- Modify Camera Privilege Group Settings
- Assign Camera to the Permission Group

When a new user group is created, its members do not have privileges to any camera or device. All cameras are listed under 'Unprivileged Cameras'. Licensed cameras will have a different icon representation than unlicensed cameras. Administrators (i.e. the user *admin*) assign cameras to camera privilege groups based on the selected user group.

TO CREATE A CAMERA PRIVILEGE GROUP

1. In the **Users / Privileges** Tab, under the user group you wish to assign devices, select the **Camera Privileges** node.
   All cameras appear under the group 'Unprivileged Cameras'.
   - To see a preview of the camera image, click the camera thumbnail icon.
   - To filter the camera list displayed, enter a keyword or phrase in the *Filter* text box.

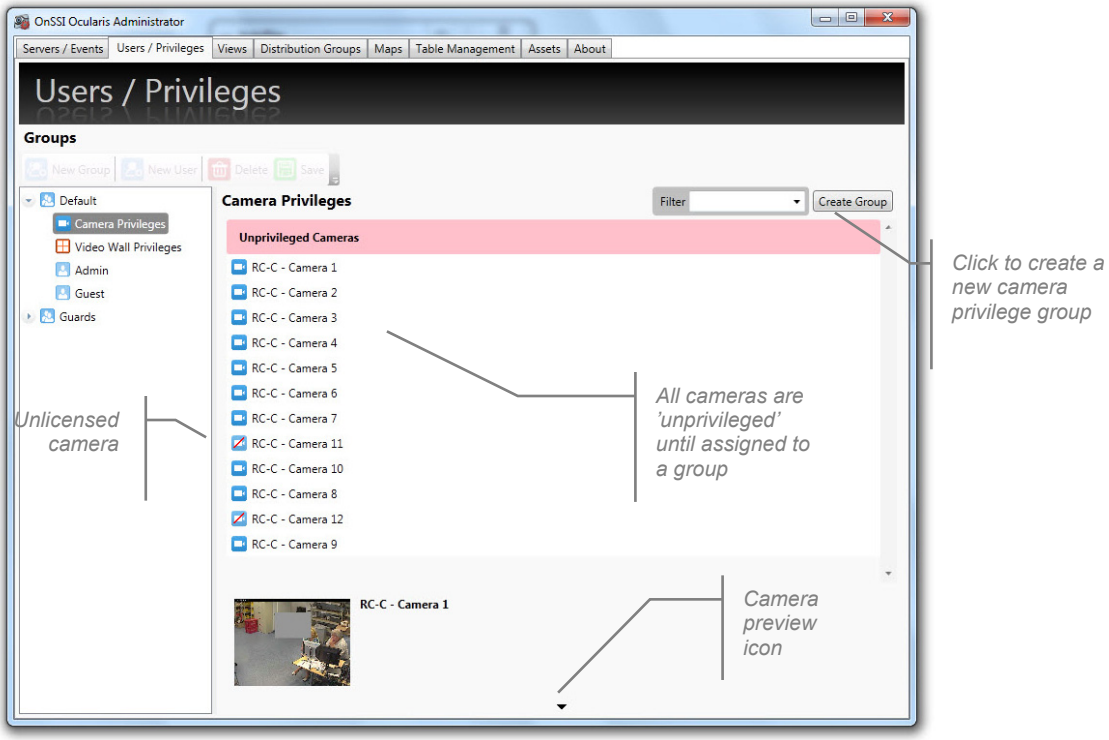


Figure 57 All Cameras Start as Unprivileged

2. In order to give members of a user group access to a camera, the camera must be assigned to a camera privilege group.

> ***Note**: Camera privilege groups set in this tab should be organized by intended functionality (vs. camera location or name) as the administrator applies camera privileges to the entire group of cameras.*

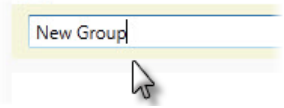
3. Click the **Create Group** button and a *New Group* entry appears.

You may now add cameras to this permission group.

TO MODIFY A CAMERA PRIVILEGE GROUP NAME

1. In the **Users / Privileges** Tab, under the user group you wish to assign devices double-click the camera privilege group name you wish to modify.

   The existing name appears in an editable text box.



2. Modify the name or replace as needed.
3. Press **[ENTER]** to save changes.

TO MODIFY CAMERA PRIVILEGE GROUP SETTINGS

1. In the **Users / Privileges** Tab, under the user group you wish to modify device settings, click the expand icon to the right of the permission group name to expand the settings parameter area.

Figure 58 Camera Privilege Group Settings

2. Modify settings based on the following:

Color

Click a color swatch on the color palette to change the color of the permission group bar displayed in this tab.

Camera Permission

For any camera placed in this group, you may apply or remove privileges as follows:

Item	***When checked, for these cameras:***
Live	
Audio In	If the device supports it, the users of this group will have the ability to listen to audio from the device.
Audio Out	If the device supports it, the users of this group will have the ability to speak to the device through its speakers.
Start Recording	This privilege allows the user to initiate manual recording while viewing live video feed from the corresponding device. Video will be recorded to the location and for the duration as defined in the NVR for that camera.
PTZ	
Presets	The users of this group will be able to direct a PTZ camera to configured preset positions.
PTZ	The users of this group will have the ability to operate pan, tilt & zoom functions on applicable cameras.
Toggle Patrol	If the camera is a PTZ camera with presets configured to patrol, this privilege allows users of this group to pause the camera at any given preset.
Browsing The checkbox under 'Browsing' will allow the camera's recorded video to be viewed by any user with Ocularis Client.	
Export Frames	The users of this group will have the ability to export still images in .jpg format from Browse mode of the *Ocularis Client* for these cameras. This will only be applicable if the value in *Browsing Limit* is not equal to 0. This parameter also controls the operator's ability to perform a snapshot of the video from Ocularis Client.

Item	*When checked, for these cameras:*
Export Video	The users of this group will have the ability to export video in both .AVI and Database Format from Browse mode of the *Ocularis Client*. This will only be applicable if the value in *Browsing Limit* is not equal to 0.
Create Bookmark	The users of this group will have the ability to export bookmarks from Browse mode of the *Ocularis Client*. This will only be applicable if the value in *Browsing Limit* is not equal to 0.
Limit	The value entered here identifies if and for how long into the past the camera's video may be viewed by this user group in Browse mode of the Ocularis Client. Valid Values include: 0 = No Browse Privilege -1 = Unlimited Browse Privilege (any available video from past recordings may be viewed) 1 through 168 = The number of hours that the users in this group may browse recorded video for the device. If the user does not have Browse privileges to a device or the user attempts to view video prior to valid browse hour times, the video will appear darkened within the *Ocularis Client*.

TO ASSIGN CAMERAS TO A PERMISSION GROUP

When a user group is first created, all cameras are grouped in an 'Unprivileged Cameras' group. This means that the cameras listed here are not accessible to the user group members at all. In order for the user group to obtain any access to a camera, a camera privilege group must be created and cameras added it to it. The camera must also be licensed in the **Servers / Events** tab. Unlicensed cameras may still be assigned to a user group in the event that, at some future date, those cameras do become licensed.

1. In the **Users / Privileges** Tab, under the user group you wish to assign devices, select the **Camera Privileges** node.
2. Select the device or devices you wish to assign to the group in the **Devices** list. Use the **SHIFT** or **CTRL** keys to select multiple items.
3. Assign cameras using either of these methods:
    a. Drag and drop the camera(s) from the **Unprivileged Cameras** group to the destination group. Cameras may also be moved between groups.

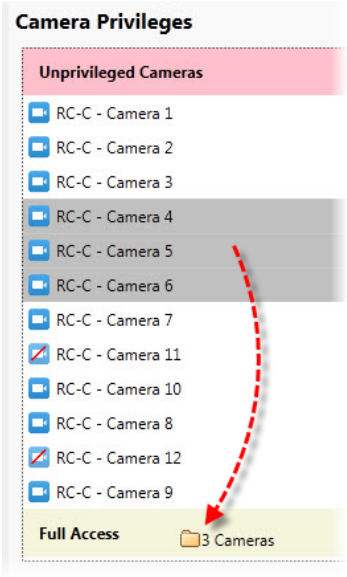


Figure 59 Drag and Drop to Assign Cameras

b. Right-click the highlighted camera(s) and select the destination camera privilege group.

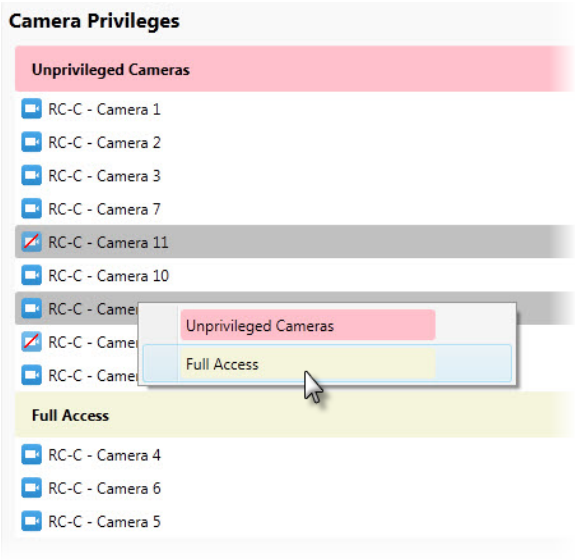


Figure 60 Right-click to Assign Cameras

To Remove a Camera From a Privilege Group

1. In the **Users / Privileges** Tab, select the group containing the device you wish to remove.
2. You can either:
   a. Drag and drop the camera to the **Unprivileged Cameras** group.
   b. Right-click the camera and select **Unprivileged Cameras**.

Video Wall Privileges

Similar to devices, users need privileges in order to view a video wall. These privileges are set in the **Users / Privileges** tab.

To Assign Access to a Video Wall To A Group

Use these steps for user accounts that will be pushing video to video walls as well as video wall user accounts that will be used on a video wall.

1. In the **Users / Privileges** Tab, select the group you wish to assign the video wall(s).
2. Select the **Video Wall Privileges** node.
3. Existing video walls are displayed. Check the checkbox for the videowall(s) to assign to this user group.

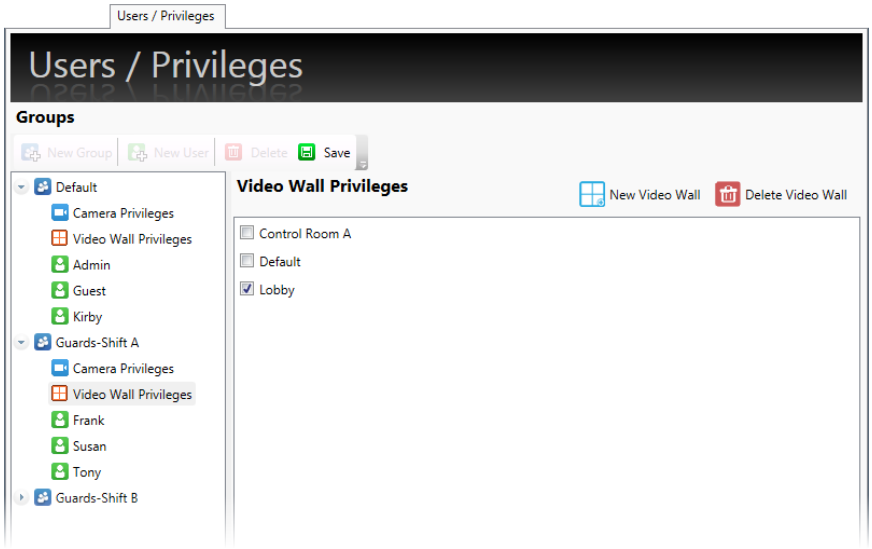


Figure 61 Check box for assigned video wall

To Remove A Video Wall From A Group

1. In the **Users / Privileges** Tab, select the group you whose video wall(s) assignment you wish to modify.
2. Select the **Video Wall Privileges** node.
3. Uncheck the video wall(s) you wish to unassign.

Video Walls

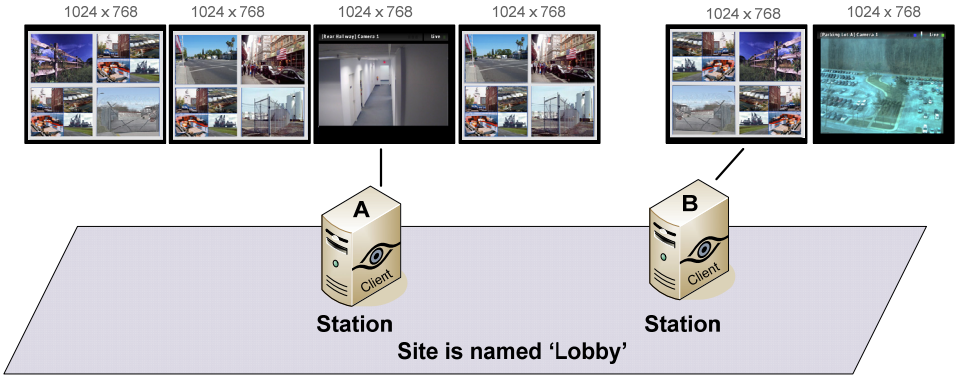
Video walls are simply a collection of monitors typically posted in a public or other observation area, with no visible keyboard attached. They are used to display video from preset cameras as well as receive video on demand, pushed there by operators or configured events. Video Walls in Ocularis are defined in the Base using the *Ocularis Administrator*. *Ocularis Client* is used to display the video wall. Remote Video Wall is an optional add-on component to Ocularis and available with *Ocularis ES*, *Ocularis LS, Ocularis CS and Ocularis IS*.

Local vs. Remote

Local video walls are those on the same station (PC) as the operator. For instance, an operator's pc may have 4 monitors attached to it with an appropriate video card. The operator can use one of the monitors to observe views and maps and the other three monitors as the video wall on which he can post video. Local video walls are available in all Ocularis feature sets.

Remote video walls are those where the video wall display monitors are not attached to the same pc as the operator. These monitors may be located in the same room or in another remote location from the operator. Remote video walls are available in the Ocularis IS, Ocularis CS, Ocularis LS and Ocularis ES feature sets.

The system administrator determines which video wall a user may push video to as well as which video wall a user account may be associated with. A *site* is synonymous with video wall. The video wall in the example shown in the graphic below has six monitors and two *stations*. Each station is a separate PC with a unique IP address. Both stations combined make up the video wall named 'Lobby'. Video wall site names are created by the administrator on the Ocularis Base. Video wall names can be any short label or description about the video wall.



Sample Video Wall

There is no technical limit to the number of screens/monitors which can encompass a video wall. There is, however, a limit to the number of screens that each Ocularis Client installation can support. Currently, each instance of Ocularis Client can support up to eight (8) monitors on a single station (or IP address). Therefore, if you wanted a video wall comprised of sixteen (16) monitors for instance, you would need at least two PCs, each with its own instance of Ocularis Client installed.

Configuring a Video Wall

Defining a video wall involves these steps:

- Creating a video wall name in the *Ocularis Administrator* **Users / Privileges** Tab.
- Assign user privileges to the video wall within the *Ocularis Administrator* **Users / Privileges** Tab.
- For automated alerts to appear on video walls in blank screen panes in sequence, include the video wall as part of the distribution group for the event in the **Distribution Groups** Tab.
- On the station(s) which includes video wall monitors, select the video wall from the 'Client Setup' function in *Ocularis Client*. See the *Ocularis Client User Manual* for more information.
- Video Walls are used in conjunction with Ocularis Maps and at least one map should be configured in order for the operator to push video to a video wall. See *Working with Maps* on page 107.

TO DEFINE A VIDEO WALL

1. In the **Users / Privileges** tab, select any user group.
2. Select the **Video Wall Privileges** node.
3. Click the **New Video Wall** button.

A new video wall site is added and available for all user groups. Modify the text (double-click the name and press ENTER) to change the site name.

TO DELETE A VIDEO WALL

1. In the **Users / Privileges** tab, select any user group.
2. Select the **Video Wall Privileges** node.
3. Select the video wall to be removed.
4. Click the **Delete Video Wall** button.

TO ASSIGN VIDEO WALL PRIVILEGES

Once a video wall site has been created, it must be assigned to a user group in order for it to be visible in the *Ocularis Client*. It should also be assigned to the user group which contains the user account(s) of the video wall station(s). This is assigned in the **Users / Privileges** Tab. For more information, see To Assign Access to a Video Wall To A Group on page 69.

OFFSETS

When multiple stations (PCs) are used in the same video call, offsets must be defined in order to prevent overlap on the operator's station. The configuration of the offsets is performed in the *Ocularis Client* 'Client Setup' screen. See the *Ocularis Client User Manual* for instructions on how to configure offsets.

Views Tab

A *View* is the fundamental display when observing video from a client application such as *Ocularis Client*. When using Ocularis Base, views are configured within *Ocularis Administrator*, in the **Views** Tab.

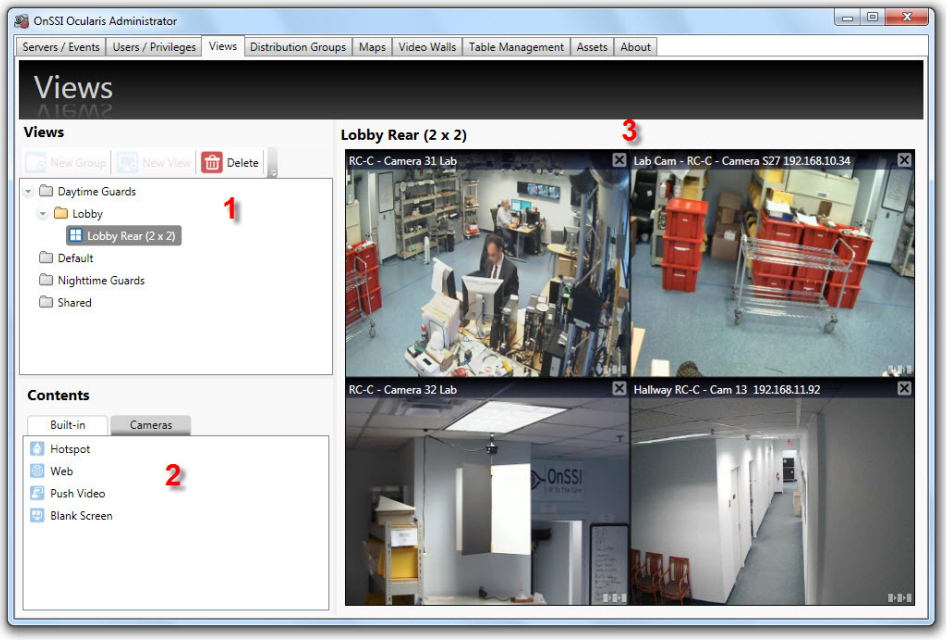


Figure 62 Views Tab

The **Views Tab** is divided into three (3) areas:

1. The **Views** list in the upper left portion of the tab contains a list of configured views organized by user group and view folders.
2. The **Contents** list in the lower left contains two tabs used to populate the various tiles of the displayed view pane.
3. The View working area can be found in the upper right area of the tab and is labeled with the view name or with **Select a View** if no view is currently selected.

Tip:	*You must have privileges to a device in order to create a view using that device. If you do not see any or a specific camera video in this pane, make sure the group you belong to contains privileges to view that camera's video.*

Resizing Panes

In the event you need to manually resize a pane in the Views tab, position the mouse on the divider between two panes until you see the mouse cursor change to a double arrow. Then you may click and drag to resize the pane.

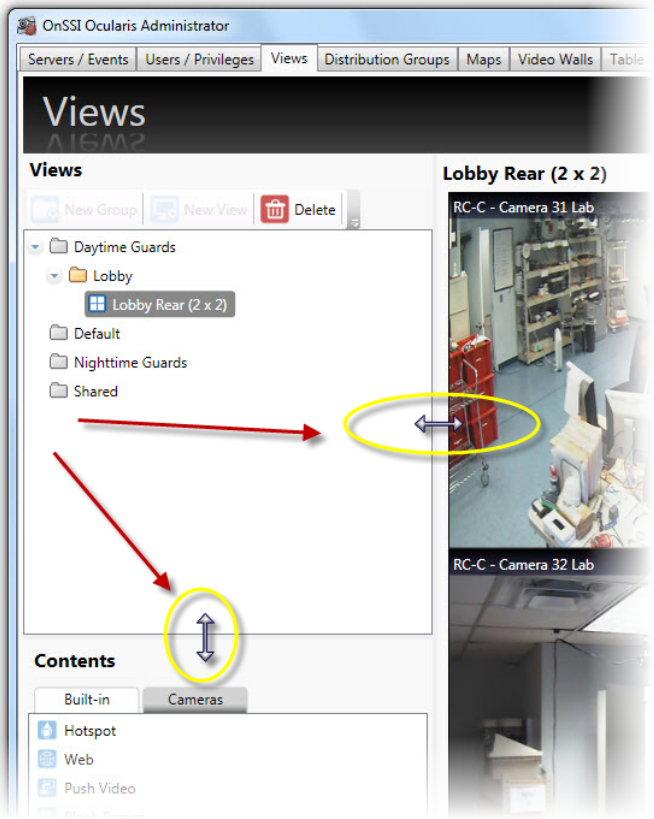


Figure 63 Resizing a Pane

View Basics

A *View* is a collection of panes or windows that display video output. There are many layout options for views.

Ocularis Base views are configured from the **Views** Tab in *Ocularis Administrator*. Administrators configure the views on a group by group basis and control which view layouts and cameras are available to users when they use *Ocularis Client*.

If a new employee joins the organization, for instance, once they are made a member of a group they inherit all Ocularis Base views for that group.

2 x 2 View *1 + 5 View*

2 + 4 View *8 x 8 View*

Figure 64 Sample views as seen via Ocularis Client

View Configurations

The following view configurations are available in Ocularis:

1 x 1	1 + 3 Wide
2 x 2	2 + 4 Wide
3 x 3	1 + 8 Wide
4 x 4	4 x 3 Wide
5 x 5	1 + 5
6 x 6	1 + 7
7 x 7	4 Top, 2 Middle, 4 Bottom
8 x 8	3 x 1

Table 1 Available View Configurations

A View consists of a varying number of *panes*. A *pane* will most often contain video output from a camera.

Contents

In addition to streaming camera video, a pane may contain other content such as a:

- Carousel
- Hot Spot
- Push Video pane
- Web Page
- Blank Screen

Carousel

A Carousel within a view pane will alternate video from camera to camera. The cameras included in the alternating output as well as the transition time between images are configured in the *Ocularis Administrator*. See *To Configure A Carousel* on page 90.

Hot Spot

A Hot Spot is a view pane dedicated to displaying images from another view pane when manually selected by the user in *Ocularis Client*. For practical purposes, hot spots are typically placed in one of the larger size view panes. See *To Configure A Hot Spot* on page 95.

Push Video

A Push Video window pane is one that is configured to accept video from another computer. Video may be “pushed” manually from one user to another user on the Ocularis Base environment. This action is performed in the *Ocularis Client*. See *To Configure Push Video* on page 96.

Web Page

A pane may contain an HTML webpage including (but not limited to): corporate websites, online maps, link collections, IP video camera configuration, flash presentation and images of a suspect, logo, map or event. See *To Configure a Web Pane* on page 97.

Blank Screen

When a pane contains a *Blank Screen* configuration, the pane will remain “blank” in the view until event driven video is triggered. The video will then be displayed in the Blank Screen pane. A benefit to using a Blank Screen is that it is attention getting. A Blank screen that suddenly displays video is easily noticed by a security guard or operator. Blank screen monitoring is supported by all Ocularis feature sets. See *To Configure a Blank Screen* on page 98 to configure a blank screen.

Content Navigation

The **Contents** list within the Views tab (see item #2 in Figure 62) contains two tabs:

- Built-in
- Cameras

Built-in

The tab labeled ‘Built-in’ displays various content available for view panes. These include: Hotspot, Web, Push Video and Blank Screen. To use any of these, simply drag and drop the item from this list to a displayed view pane.

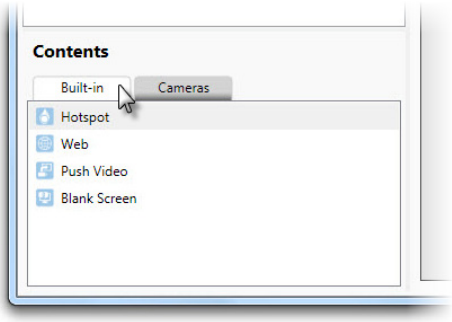


Figure 65 Built-in Tab of Contents List

Cameras

The tab labeled ‘Cameras’ displays the cameras assigned to the selected view group from the Views list above. By default, a folder labeled ‘All’ appears, listing all available cameras for the selected group in alphanumeric order.

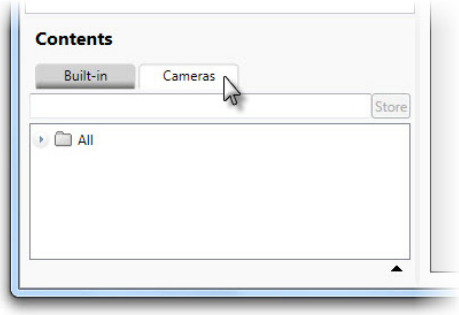


Figure 66 Cameras Tab

Expand the folder to see its contents.

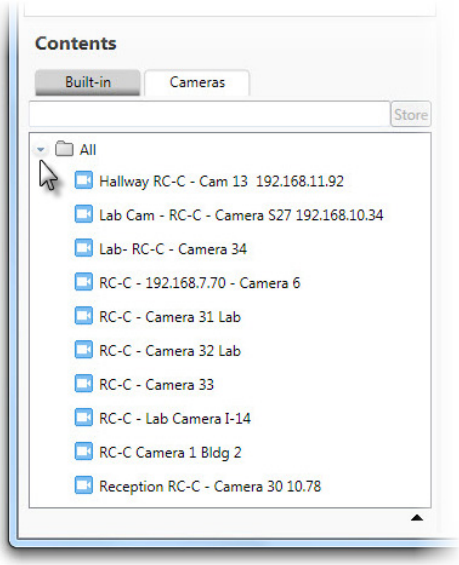

Contents
Built-in
Cameras
Store
All
Hallway RC-C - Cam 13 192.168.11.92
Lab Cam - RC-C - Camera S27 192.168.10.34
Lab- RC-C - Camera 34
RC-C - 192.168.7.70 - Camera 6
RC-C - Camera 31 Lab
RC-C - Camera 32 Lab
RC-C - Camera 33
RC-C - Lab Camera I-14
RC-C Camera 1 Bldg 2
Reception RC-C - Camera 30 10.78

Figure 67 All Cameras for the selected View Group

Camera Preview

In many cases, you may not know the image of a camera simply by looking at its name. In these cases, you may invoke a *Camera Preview* for a selected camera.

TO PREVIEW A CAMERA IN THE VIEWS TAB

1. In the Views tab, select the View Group for cameras you wish to preview.
2. Click the **Cameras** tab in the Contents list.
3. Expand a camera folder and select a camera.
4. Click the *Expand Camera Preview* icon.

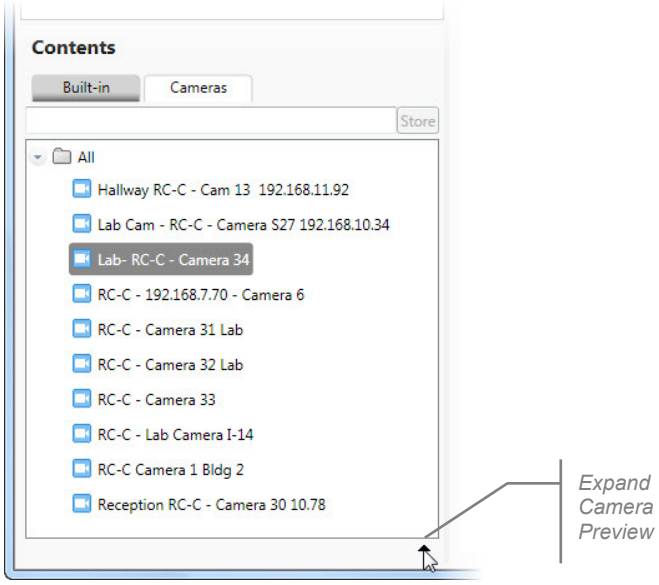


Figure 68 Expand Camera Preview Icon

A camera preview thumbnail appears below the camera list. The camera list will remain in preview mode until you collapse the preview. Select another camera and the preview thumbnail will update.

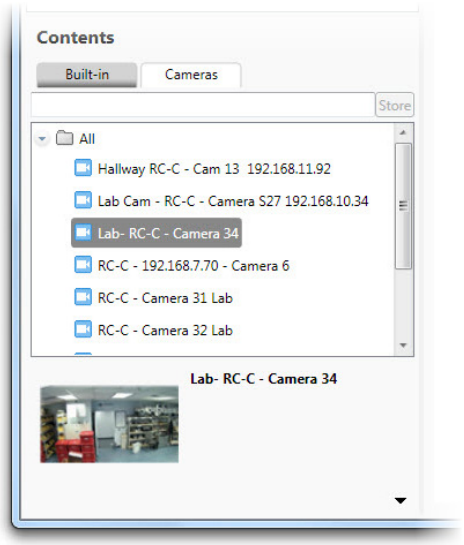


Figure 69 Camera Preview Thumbnail

5. Collapse the camera preview by clicking the *Collapse Camera Preview* icon.

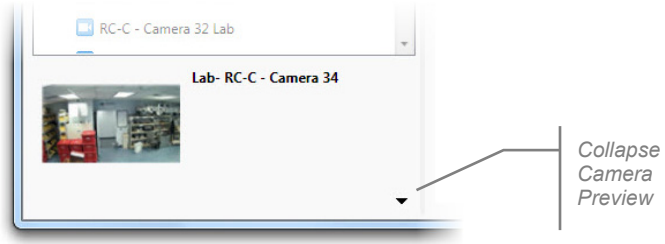


Figure 70 Collapse Camera Preview Icon

Camera Filter

The camera list in the Views Tab (and Maps Tab) may be quite lengthy depending on the installation. The list can contain hundreds or thousands of cameras making locating just the one you want a time consuming process. Luckily, you have the ability to filter the list of cameras based on a keyword and also to store this search for later use.

To Use the Camera Search Filter

1. In the Views tab, select the View Group you wish to work with.
2. Click the **Cameras** tab in the Contents list.
3. In the *Camera Search* text box, type in a keyword to be used as the camera filter.

   Keywords are not case sensitive and filter based upon the camera name as inherited by the recorder. (Therefore, it is important to know and understand the naming structure of the recorder cameras). If, for instance, you named your cameras using the manufacturer name, you may use this as the keyword. Or perhaps the cameras were named based on their location (Parking Lot A, Parking Lot B, etc.). Use any portion of the camera name to filter the list.
4. As you begin to type the keyword, the list will update.

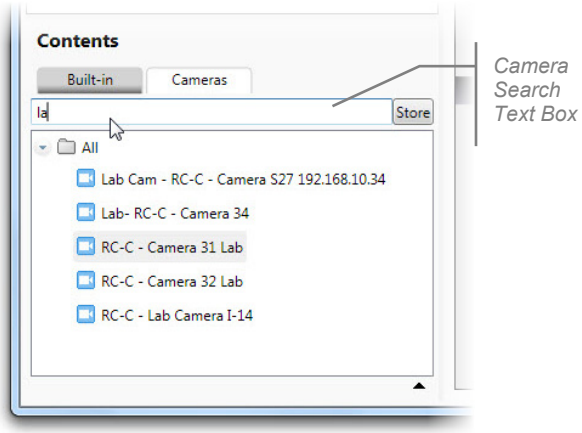


Figure 71 Camera Search box

5. You can use the list as is (i.e. drag and drop displayed cameras).
6. If you would like to store the list for later use or in the Maps tab, click the **Store** button.

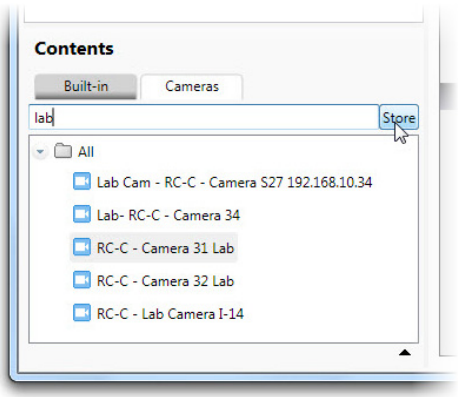


Figure 72 Click Store to Save Search Filter

7. A new folder is created containing the subset of cameras as filtered in step 3. This filter can now be shared:
    - With other view groups
    - In the Maps Tab

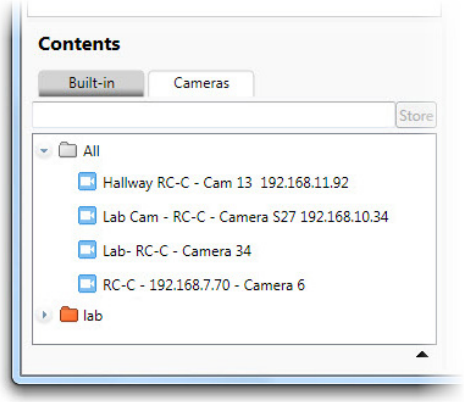


Figure 73 Example of stored camera filter 'lab'

8. Repeat these steps to add additional camera search filters.

Now you may use these stored folders to easily locate cameras as defined by the keyword filter.

> ***Note**:*
> *The cameras displayed in stored camera folders will be filtered further based upon the user group privileges assigned. If, for instance, the keyword search is on the word 'lab' and the Daytime Guards have access to 10 cameras which include the keyword 'lab' but the Nighttime Guards only have access to 5 of these cameras, only the 5 cameras will be available to the Nighttime Guards.*

View Organization

Views are organized first by user group (as defined in the **Users / Privileges** Tab) and then by *view group* or *folder*. A view group may contain multiple folders and a folder may contain multiple views. A folder may also contain multiple folders (or nested folders). A folder called 'Shared' appears in all Ocularis installations. This folder contains views that may be shared across multiple user groups.

Creating Views

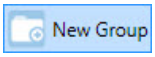
Consider the users and their user groups as they are intended to use the system. Some users will require certain views to certain cameras. Other users may require access to different cameras in different locations. The system administrator should take into account the user role and job function when creating views in the *Ocularis Administrator*.

As discussed previously, views are assigned to user groups but are organized by folders. Therefore, you must first create a folder or view group and then you may create a view. Group Administrators may only create, edit or delete views within their own user group.

Private and Shared Views

Views may be created for an individual user group or they may be shared across user groups. Consider, however, that when you create a view, if you think that it will ever need to be shared with more than one user group, to create it as a shared view. This will make it easier, later on, to allow multiple users group access to a shared view. Group Administrators, however, may view shared views for their user group, but they may not edit them or create new shared views. Only the *admin* user can create a shared view.

TO CREATE A FOLDER FOR A VIEW GROUP

1. In the **Views** Tab, select either:
   - the user group for which you would like to create a folder
   - the Shared folder
   - an existing folder beneath a user group or Shared group and create a nested folder beneath it.
2. Click the **New Group** button. 

3. A folder is created labeled “New Group”.

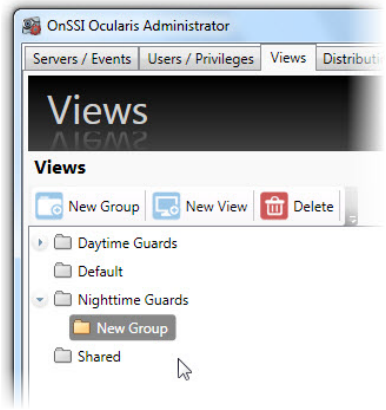


Figure 74 Create a View Group

TO MODIFY THE NAME OF A VIEW GROUP

1. In the **Views** Tab, double-click the group folder you wish to rename.

   The folder name becomes highlighted.
2. Type the new name for the folder.
3. Press [**ENTER**] to accept changes.

TO DELETE A FOLDER WITHIN A GROUP

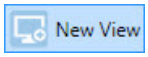
1. In the **Views** Tab, select the folder which you would like to delete.
2. Click the **Delete** button.

An "*Are you sure you want to delete this view group?*" prompt appears.

3. Click **Yes** to delete.

TO CREATE A VIEW WITHIN A FOLDER/VIEW GROUP

Once view folders / view groups are created, views may be added to them.

1. In the **Views** Tab, select the folder for which you would like to create the view. If you intend on sharing this view with multiple groups, create the view under the 'Shared' folder hierarchy.
2. Click the **New View** button. 

   The view layout pop-up appears.

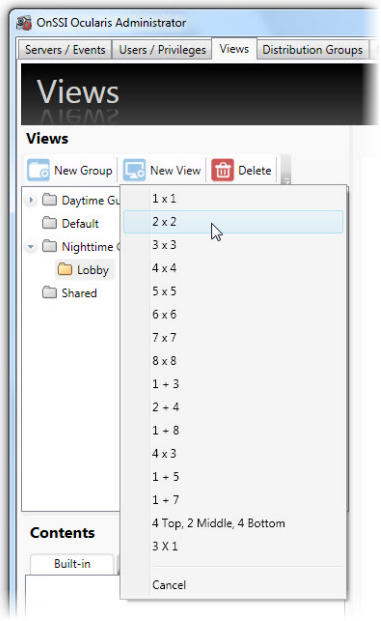


Figure 75 Create View - View Layouts

3. Select a layout from the list of View Configurations.
   A blank template for the layout appears in the View working area and a view called "New View(*layout*)" is created.

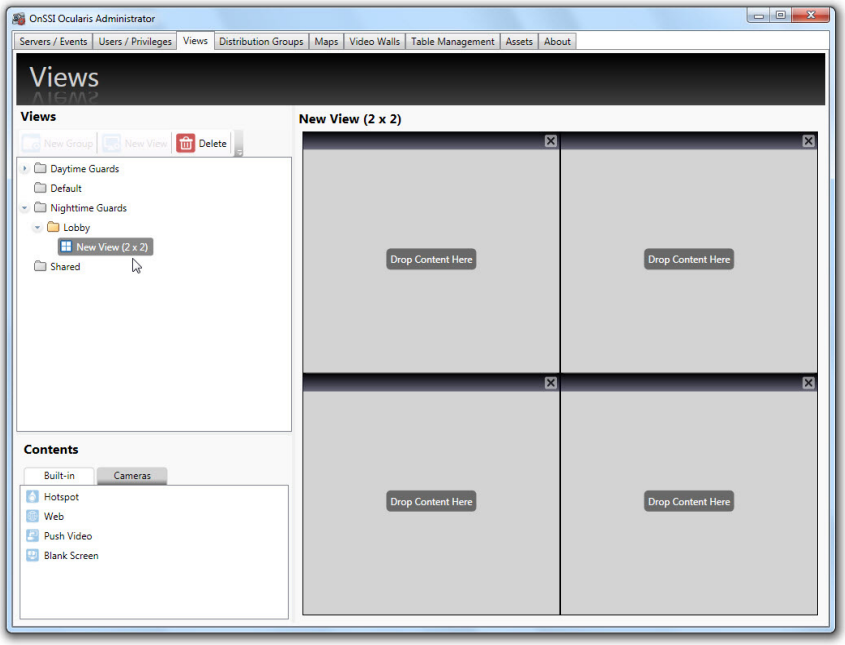


Figure 76 Creating a New View for a Single User Group

In the event that the view is to be shared between multiple user groups, be sure to create the view underneath the 'Shared' view group hierarchy. For example:

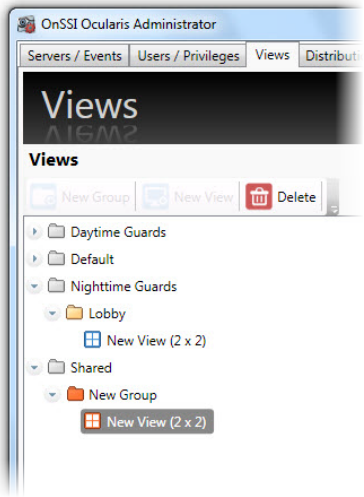


Figure 77 Shared Views

Notice in Figure 77, Shared items (folders and views) are shown in the color orange.

4. With the desired new view selected, populate each view pane by dragging and dropping a camera or other pane content from the Contents list onto a pane.

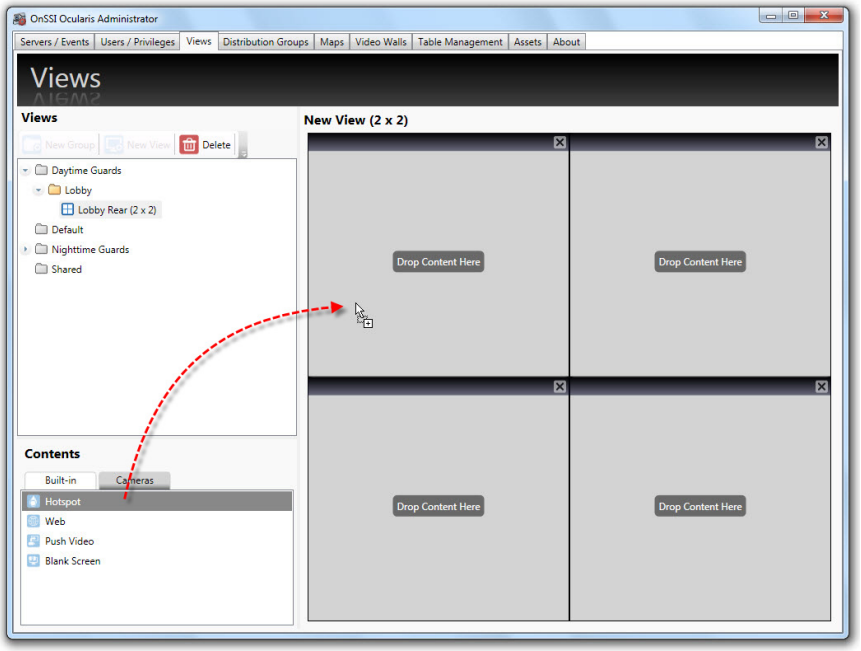


Figure 78 Example: Drag a Hotspot to a View Pane

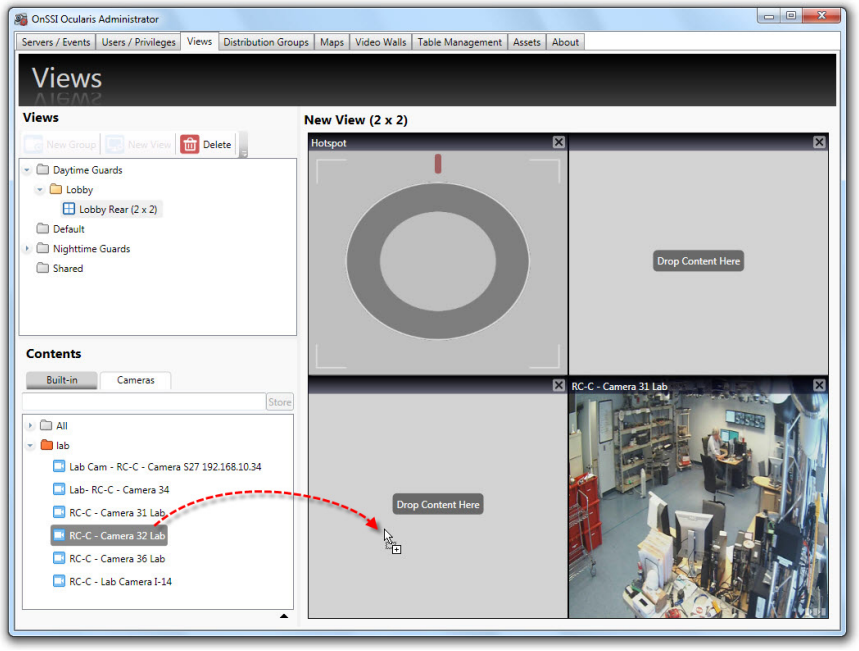


Figure 79 Example: Drag a Camera to a View Pane

Changes to views are automatically saved.

View Modification

View modification is limited to renaming the view or changing the contents of a pane within the view. Reconfiguring the view layout is not available. Therefore if, for instance, you need to change the view layout from a 2 x 2 to a 3 x 3, you should delete the 2 x 2 view and create the 3 x 3 view from scratch.

To Rename a View

1. In the Views Tab, double-click the view you would like to rename.
2. Type the new name for the view.
3. Press [**ENTER**].

TO DELETE A VIEW

1. In the **Views** Tab, select the view which you would like to delete.
2. Click the **Delete** icon.

An "*Are you sure that you want to delete this view?*" prompt appears.
3. Click **Yes** to delete the view.

TO MODIFY CONTENTS OF A VIEW PANE

1. In the **Views** Tab, select the view which you would like to modify.
2. To change the configuration of an existing pane, click the pane to view the pane configuration settings. Make changes as required.
3. To replace a pane with a different component (camera, carousel, hot spot, etc.) you may:
   - Remove the pane content by clicking the **Clear View** icon in the pane.

Figure 80 Click Clear View to remove pane contents

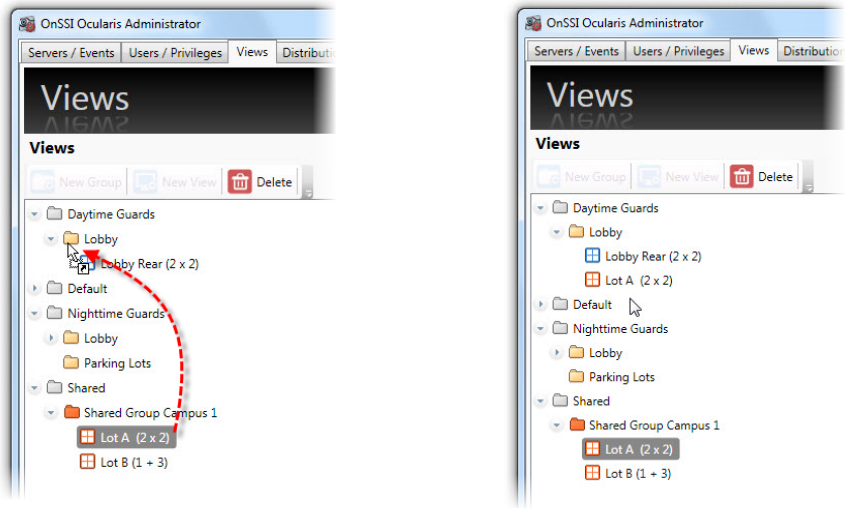
   - Replace the pane contents by dragging & dropping a camera thumbnail or built-in type onto the pane.

Shared Views

Once a shared view is created underneath the Shared folder, additional steps must be taken in order to share it. It must be assigned to the desired user group(s).

TO SHARE A VIEW WITH A USER GROUP

1. In the **Views** Tab, expand both the view you would like to share under the Shared folder as well as the User Group (and its corresponding view group) that you wish to share the view with.
2. Drag and drop the view from the Shared view group to the view folder for the desired user group. Notice how the mouse cursor changes when it is positioned correctly over the destination folder.



Drag and drop to share a view *Shared views displayed in orange*

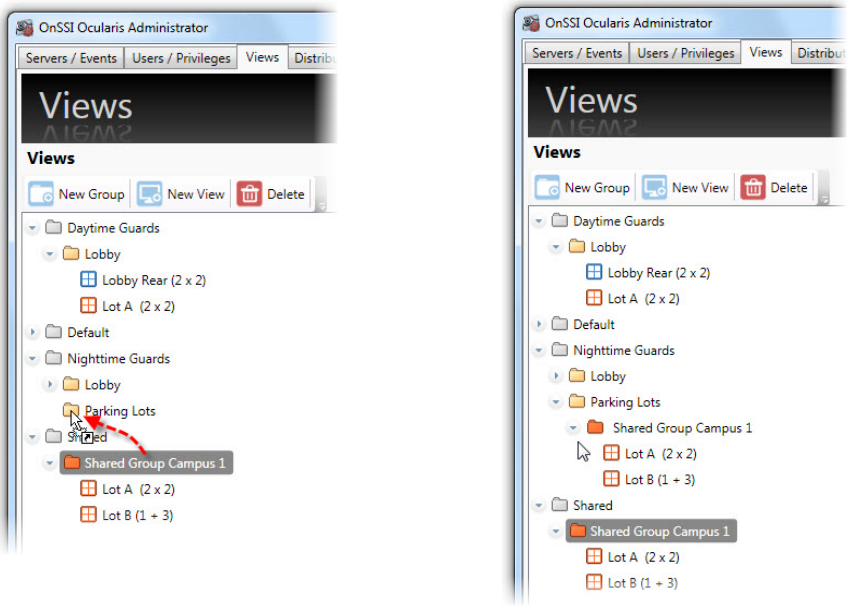
Figure 81 Sharing Views

3. Repeat this procedure to share this view with other user groups or to share other shared views with any user group.

Additionally, entire groups of shared views may also be shared, making it easy to share multiple views in one step.

TO SHARE A VIEW GROUP WITH A USER GROUP

1. In the **Views** Tab, expand both the view group/folder you would like to share under the Shared folder as well as the User Group (and its corresponding view group) that you wish to share the view group with.
2. Drag and drop the view group (folder) from the Shared view group to the view folder for the desired user group. Notice how the mouse cursor changes when it is positioned correctly over the destination folder.



Drag and drop to share a view group *Shared Groups displayed in orange*

Figure 82 Sharing View Groups

3. Repeat this procedure to share this view group with other user groups or to share other shared views with any user group.

Modifying Shared Views

Shared views may be modified the same way as private views (see *To Modify Contents of a View Pane* on page 85). However, only the *admin* user can modify a shared view and it can only be modified when selected under the Shared view group. When a shared view is selected under a user group, a 'padlock' icon appears over the pane to indicate that the view may not be modified.

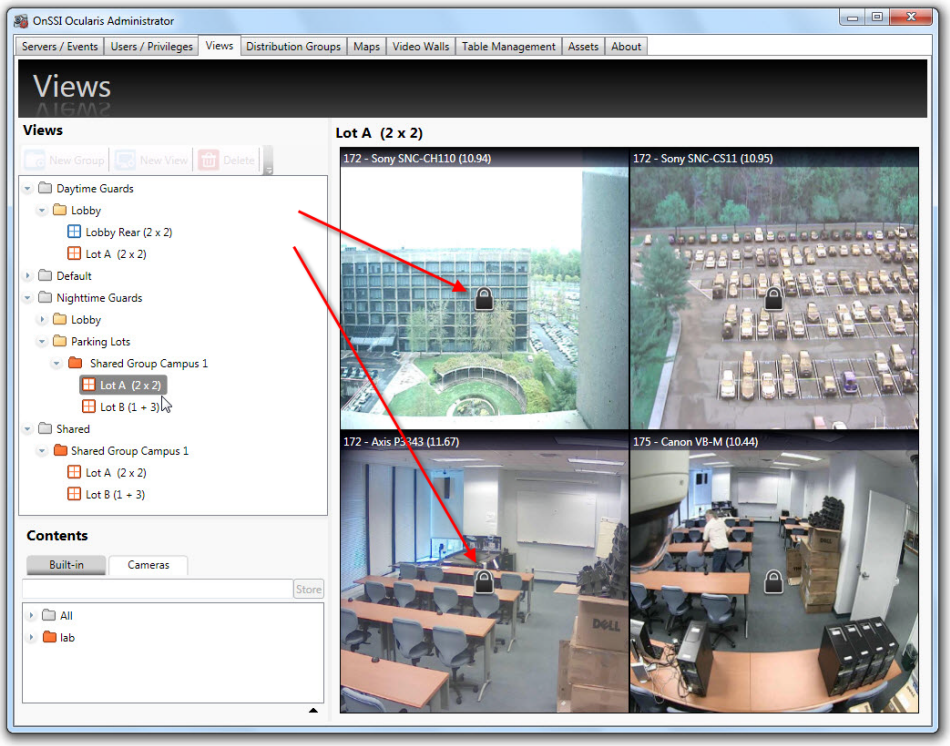


Figure 83 Padlock indicates view may not be modified in this selection

Changes made to a shared view will be reflected in all individual user groups who have permission to access that view.

Configuring View Content Types

Once view panes are populated with content, specific parameters may be set for each content type. The following section will discuss:

- Camera Configuration
- Carousel Configuration
- Hot Spot Configuration
- Push Video Configuration
- Web Page Configuration
- Blank Screen Configuration

Camera Output Configuration

Actual video configuration for camera resolution and recording is done on the recorder. Configuration for camera output here refers to how the camera's video appears in the *Ocularis Client*.

TO CONFIGURE CAMERA OUTPUT

1. In the **Views** Tab, select the view which contains the pane with the camera video you wish to configure. (For information on creating a view see *To Create A View within a Folder* on page 82.)
2. Click on the pane with the video you wish to configure.

   A *Viewport Properties* pop-up appears corresponding to the type of pane content selected (in this case, a camera). View pane contents with a single camera is considered a one camera carousel. (More details on carousels in the next section).

Figure 84 Click on the pane to modify parameters

3. You have the option to modify the following *Camera Overlay Parameters*:

Aspect	Useful for wide screen video output, the default option, **Fit to Window** will cause the video to be stretched to fit the window pane and may cause the video to appear slightly distorted. The option **Keep Original** may result in black vertical or horizontal bars surrounding the video when viewed in *Ocularis Client*.
Framerate	This setting is the framerate for the camera while viewing Live video in *Ocularis Client*. Available options are: **Full** (default), **Medium** or **Low**. Save bandwidth by selecting Medium or Low.

Quality	Options are: **Original**, **Super High**, **High**, **Medium**, and **Low**. This setting applies to Live video. To save on bandwidth, lower the image quality. The video from the camera is re-encoded to a JPEG format on the server before being sent to *Ocularis Client*. The default quality setting, **Original**, provides full quality of the original video. **Low** quality re-encodes the image to an output width of 160 pixels and a JPEG quality level of 20%.
Keep when maximized	When an individual pane is maximized in *Ocularis Client*, the default is to display the video in its Original quality. Check this box to maintain the quality parameters set here when the pane is maximized to full screen.

4. To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

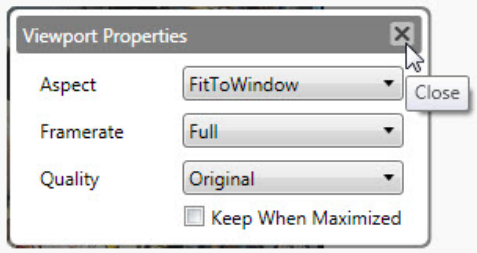


Figure 85 Close using the Close icon

Camera Overlay Parameters

The settings discussed above are also displayed as overlay parameters when the mouse is passed over the pane in the Views tab.

Figure 86 Overlay Parameters

Carousel Configuration

Carousel configuration includes: identifying which cameras are to be used in the Carousel, the video parameters as displayed in Ocularis Client and the image's dwell time.

TO CONFIGURE A CAROUSEL

1. In the **Views** Tab, select the view (or create a new view) which contains the pane with the carousel you wish to configure. (For information on creating a view see *To Create A View within a Folder* on page 82.)
2. Assign one camera to the pane (drag and drop) which will display the carousel.
3. Click the **Carousel Edit** icon found in the overlay section of the pane (lower right).

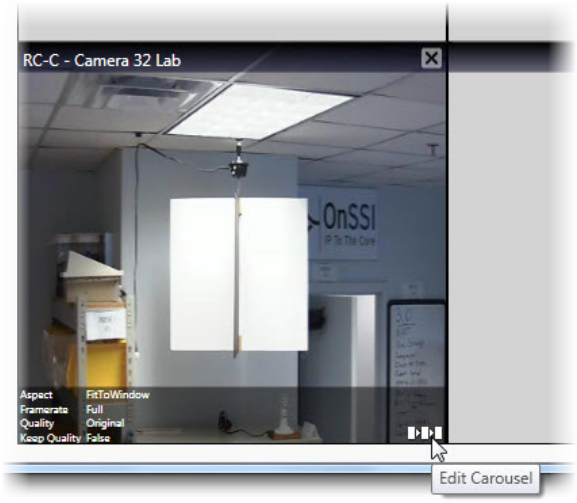


Figure 87 Carousel Edit icon

A *Carousel Editor* pop-up appears.

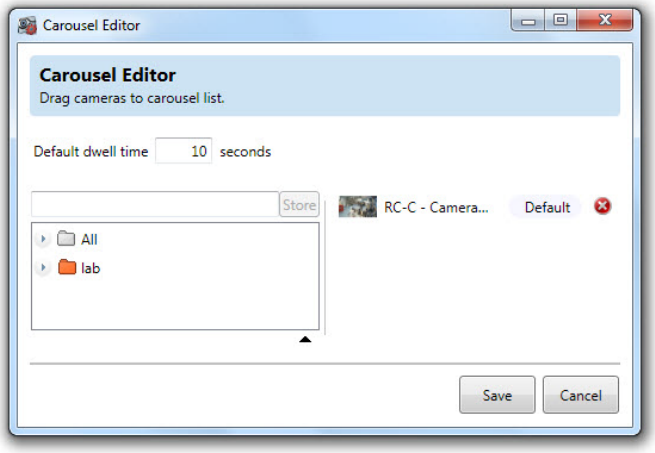
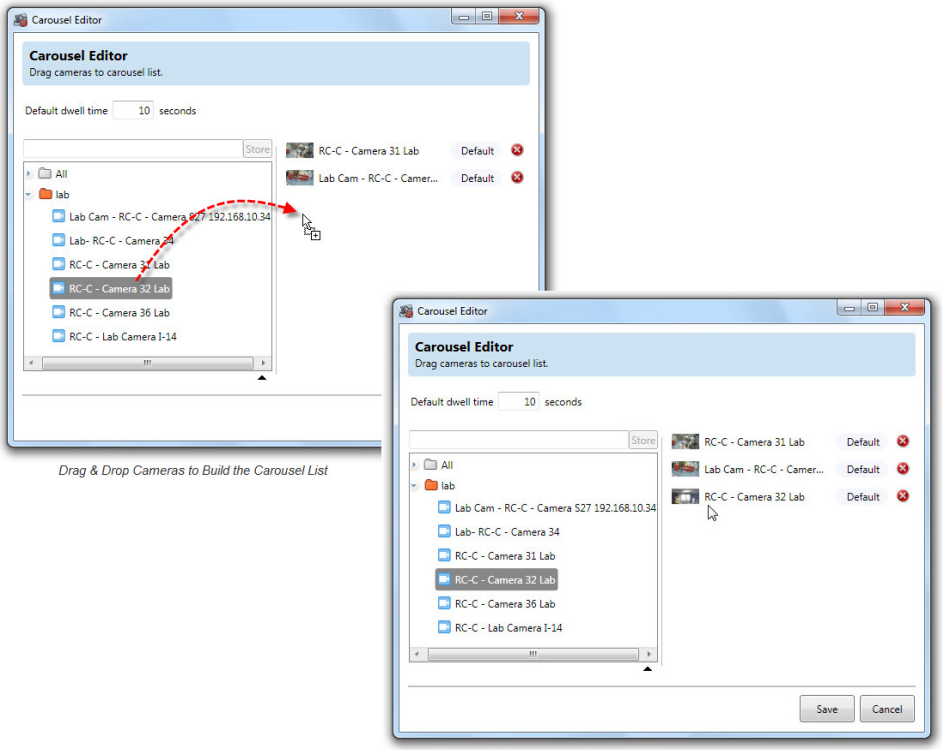


Figure 88 Carousel Editor

The goal is to create a list of the cameras you wish to display in the carousel in the camera list on the right of the pop-up. You have the same tools in this dialog to locate cameras as you do when building a view. (See *Camera Preview* on page 77 and *Camera Filter* on page 78).

> ***Tip***: *You may widen the dialog box to be able to read lengthy camera names more easily.*

4. Once you locate the desired camera in the camera list on the left, drag and drop the camera to the camera list on the right.



Drag & Drop Cameras to Build the Carousel List

Figure 89 Creating a carousel list

Carousel Order

The progression of video will go from each camera in the order listed here.

5. If you wish to reorder, simply drag and drop the camera to the correct order.

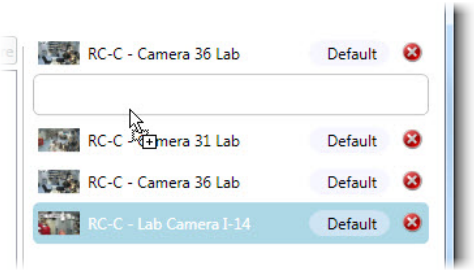


Figure 90 Reorder a Camera in a Carousel

Dwell Time

Dwell Time is the amount of time, in seconds, that camera video is displayed in the *Ocularis Client* before switching to the next camera in the list. The default Dwell Time is 10 seconds.

6. You may modify the default dwell time for all cameras shown by simply changing the number in the **Default dwell time** field. (see Figure 88).

7. If you want a single camera to have a different dwell time than the default, click the **Default** button next to the camera name. A slider becomes visible.

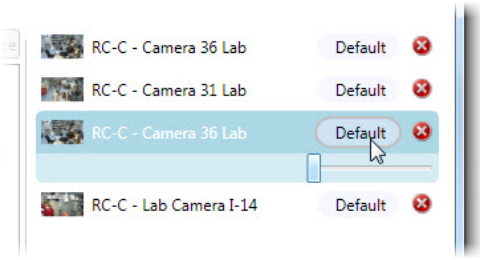


Figure 91 Change the Default Dwell Time

8. Drag the slider left or right to see the amount of seconds change. Stop when you arrive at the desired amount.

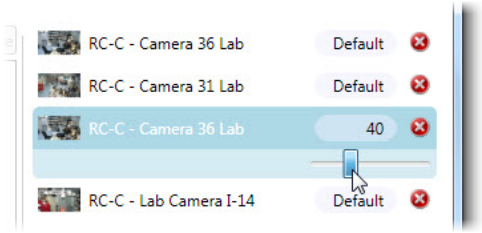


Figure 92 Default Dwell Time

9. You may do this for each and every camera listed.

10. To remove a camera from the carousel list, click the Delete icon to the right of the camera name.

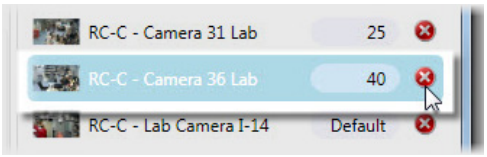


Figure 93 Remove a Camera from the Carousel List

11. When the carousel configuration is complete, click **Save**.

Figure 94 A configured carousel in the Views Tab

The **Views** tab shows the carousel with left and right arrows. The top of the pane indicated the number of cameras in the carousel (e.g. “Carousel of 4 entries”). Click the left or right arrow to scroll through the display of the cameras you selected for the carousel You may set the Camera Overlay Parameters (as shown on page 89) for the pane which displays this carousel.

TO REORDER CAMERAS IN A CAROUSEL

1. In the **Views** Tab, select the view with the carousel you wish to configure.
2. Click the **Carousel Edit** icon found in the overlay section of the carousel pane (lower right).
3. In the *Carousel Editor* pop-up, drag and drop the cameras listed to the desired order. (see Figure 90*)*.
4. Repeat for all cameras you wish to reorder.
5. Click **Save** when done.

TO REMOVE CAMERAS FROM A CAROUSEL

1. In the **Views** Tab, select the view with the carousel you wish to configure.
2. Click the **Carousel Edit** icon found in the overlay section of the carousel pane (lower right).
3. Locate the camera you wish to remove.
4. Click the **Remove Camera** icon. (see Figure 93)
5. Repeat for all cameras you wish to remove.
6. Click **Save** when done.

TO CHANGE OR VIEW THE DWELL TIME FOR AN INDIVIDUAL CAMERA

1. In the **Views** Tab, select the view with the carousel you wish to configure.
2. Click the **Carousel Edit** icon found in the overlay section of the carousel pane (lower right).
3. Locate the camera whose dwell time you wish to modify.
4. Click the **Dwell Time** button (see Figure 91).
5. When the dwell time slider appears (Figure 92), drag it left or right to modify the dwell time.
6. Repeat for each camera whose dwell time you wish to modify.
7. Click **Save** when done.

TO CONFIGURE VIDEO DISPLAYED IN A CAROUSEL

Video parameters displayed while viewing the carousel in Ocularis Client may be adjusted, similar to adjusting video for a single camera.

1. In the **Views** Tab, select the view which contains the pane with the carousel.
2. Click on the pane video.
3. In the resulting *Viewport Properties* dialog, modify the parameters as defined in the following table. The settings will apply to all camera video displayed in the carousel.

Aspect	Useful for wide screen video output, the default option, **Fit to Window** will cause the video to be stretched to fit the window pane and may cause the video to appear slightly distorted. The option **Keep Original** may result in black vertical or horizontal bars surrounding the video when viewed in *Ocularis Client*.
Framerate	This setting is the framerate for the camera while viewing Live video in *Ocularis Client*. Available options are: **Full** (default), **Medium** or **Low**. Save bandwidth by selecting Medium or Low.
Quality	Options are: **Original**, **Super High**, **High**, **Medium**, and **Low**. This setting applies to Live video. To save on bandwidth, lower the image quality. The video from the camera is re-encoded to a JPEG format on the server before being sent to *Ocularis Client*. The default quality setting, **Original**, provides full quality of the original video. **Low** quality re-encodes the image to an output width of 160 pixels and a JPEG quality level of 20%.
Keep when maximized	When an individual pane is maximized in *Ocularis Client*, the default is to display the video in its Original quality. Check this box to maintain the quality parameters set here when the pane is maximized to full screen.

4. To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

Hot Spot Configuration

Administrators can configure the quality of the camera video displayed in a Hot Spot pane.

TO CONFIGURE A HOT SPOT

1. In the **Views** Tab, select the view which contains the Hot Spot. (For information on creating a view with a hot spot, see *To Create A View within a Folder* on page 82.)
2. Click on the pane with the hot spot.

   A *Hotspot Properties* pop-up appears.

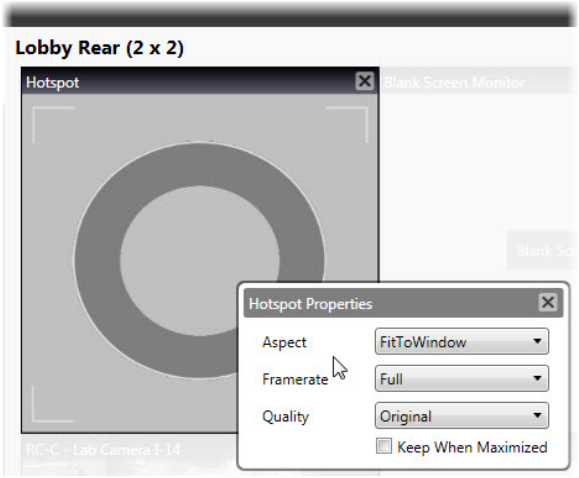


Figure 95 Configuring Hot Spot Output

3. You have the option to modify the following:

Aspect	Useful for wide screen video output, the default option, **Fit to Window** will cause the video to be stretched to fit the window pane and may cause the video to appear slightly distorted. The option **Keep Original** may result in black vertical or horizontal bars surrounding the video when viewed in *Ocularis Client*.
Framerate	This setting is the framerate for the camera while viewing Live video in *Ocularis Client*. Available options are: **Full** (default), **Medium** or **Low**. Save bandwidth by selecting Medium or Low.
Quality	Options are: **Original**, **Super High**, **High**, **Medium**, and **Low**. This setting applies to Live video. To save on bandwidth, lower the image quality. The video from the camera is re-encoded to a JPEG format on the server before being sent to *Ocularis Client*. The default quality setting, **Original**, provides full quality of the original video. **Low** quality re-encodes the image to an output width of 160 pixels and a JPEG quality level of 20%.
Keep when maximized	When an individual pane is maximized in *Ocularis Client*, the default is to display the video in its Original quality. Check this box to maintain the quality parameters set here when the pane is maximized to full screen.

4. To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

Push Video Configuration

Push Video panes are used in *Ocularis Client* to manually push video from one logged in Ocularis Base user to another logged in user. The Push Video function uses port 7008. Push video with Ocularis is supported with all Ocularis feature sets.

TO CONFIGURE PUSH VIDEO

1. In the **Views** Tab, select the view which contains the Push Video Port pane. (For information on creating a view see *To Create A View within a Folder* on page 82.)
2. Click on the Push Video pane.

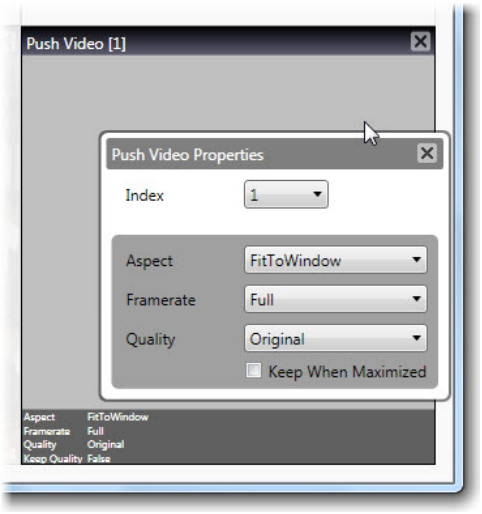


Figure 96 Configuring a Push Video Pane

3. You have the option to modify the following:

Window Index	If there are multiple panes configured for Push Video this index determines the order in which pushed video will appear in the view.
Aspect	Useful for wide screen video output, the default option, **Fit to Window** will cause the video to be stretched to fit the window pane and may cause the video to appear slightly distorted. The option **Keep Original** may result in black vertical or horizontal bars surrounding the video when viewed in *Ocularis Client*.
Framerate	This setting is the framerate for the camera while viewing Live video in *Ocularis Client*. Available options are: **Full** (default), **Medium** or **Low**. Save bandwidth by selecting Medium or Low.
Quality	Options are: **Original**, **Super High**, **High**, **Medium**, and **Low**. This setting applies to Live video. To save on bandwidth, lower the image quality. The video from the camera is re-encoded to a JPEG format on the server before being sent to *Ocularis Client*. The default quality setting, **Original**, provides full quality of the original video. **Low** quality re-encodes the image to an output width of 160 pixels and a JPEG quality level of 20%.
Keep when maximized	When an individual pane is maximized in *Ocularis Client*, the default is to display the video in its Original quality. Check this box to maintain the quality parameters set here when the pane is maximized to full screen.

4. To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

Web Configuration

In addition to camera video, panes may be populated by an HTML page accessible via URL or IP Address. Typical examples of these include:

- Company websites or logos
- Online or static maps
- Link collections
- IP Camera configuration page

> ***Note**:*
> *Panes with web pages or images may not be maximized in Ocularis Client. For web pages, we recommend using a large size pane or even a 1 x 1 pane.*

TO CONFIGURE A WEB PANE

1. In the **Views** Tab, select the view which contains the Web Page. (For information on creating a view see *To Create A View within a Folder* on page 82.)
2. Click on the pane with the Web Page.

   A *Web Properties* pop-up appears.

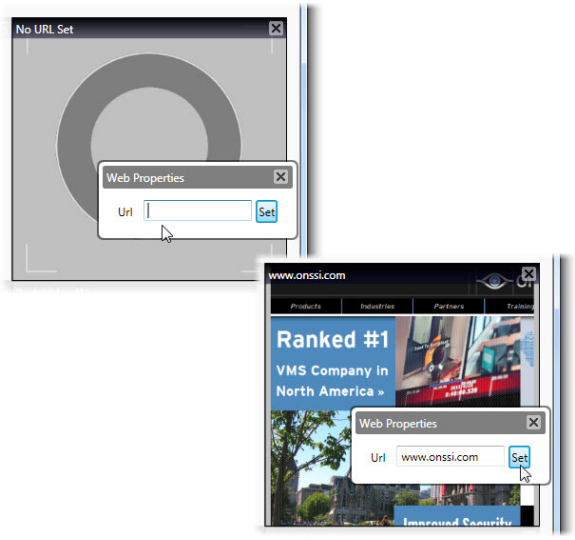


Figure 97 Configuring a Web Page Pane

3. Type in the URL or IP Address for the content to be displayed. You will see a preview of the page.
4. To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

The web page will now appear in the *Ocularis Client* and the user will be able to navigate the page using embedded links.

You may also link to an image located on the network or internet by inserting the file's full path and filename in the Url field.

Blank Screen Configuration

As the name indicates, the view pane configured with a Blank Screen remains 'blank' until populated by video triggered by an event. The event trigger is configured in *Ocularis Administrator* and is discussed in Simple Event Rules on page 37.

TO CONFIGURE A BLANK SCREEN

1. In the **Views** Tab, select the view which contains the Blank Screen. (For information on creating a view see *To Create A View within a Folder* on page 82.)
2. Click on the pane with the Blank Screen. A *Blank Screen Properties* pop-up appears.

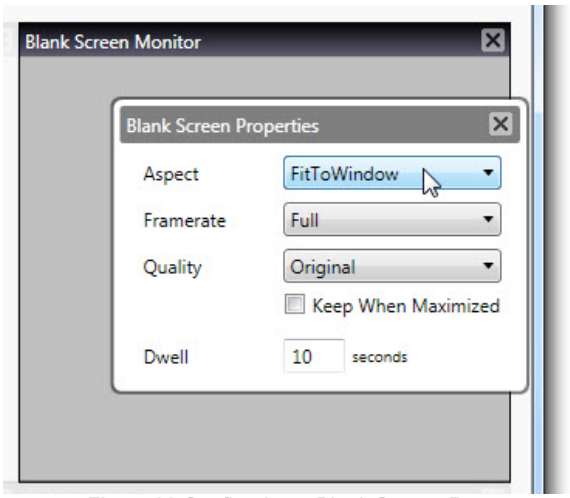


Figure 98 Configuring a Blank Screen Pane

3. You have the option to modify the following:

Aspect	Useful for wide screen video output, the default option, **Fit to Window** will cause the video to be stretched to fit the window pane and may cause the video to appear slightly distorted. The option **Keep Original** may result in black vertical or horizontal bars surrounding the video when viewed in *Ocularis Client*.
Framerate	This setting is the framerate for the camera while viewing Live video in *Ocularis Client*. Available options are: **Full** (default), **Medium** or **Low**. Save bandwidth by selecting Medium or Low.
Quality	Options are: **Original**, **Super High**, **High**, **Medium**, and **Low**. This setting applies to Live video. To save on bandwidth, lower the image quality. The video from the camera is re-encoded to a JPEG format on the server before being sent to *Ocularis Client*. The default quality setting, **Original**, provides full quality of the original video. **Low** quality re-encodes the image to an output width of 160 pixels and a JPEG quality level of 20%.
Keep when maximized	When an individual pane is maximized in *Ocularis Client*, the default is to display the video in its Original quality. Check this box to maintain the quality parameters set here when the pane is maximized to full screen.
Dwell	This is the amount of time in seconds that video will be displayed in a Blank Screen pane; applies to low and medium priority only.

4. To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

Assets Tab

The **Assets** Tab displays the centralized repository of all graphic images and audio files used in Ocularis Base. Administrators import graphic files and icon assets in this tab that may be used to configure Ocularis Maps.

Each organization will have a unique set of images and there is no limit to the amount of images that may be imported. An unlimited amount of audio files for use in alert notifications are also imported here.

Graphic images are imported through the Assets Tab and configured in the Maps Tab.

Audio files are imported through the Assets Tab and configured in the Server / Events Tab.

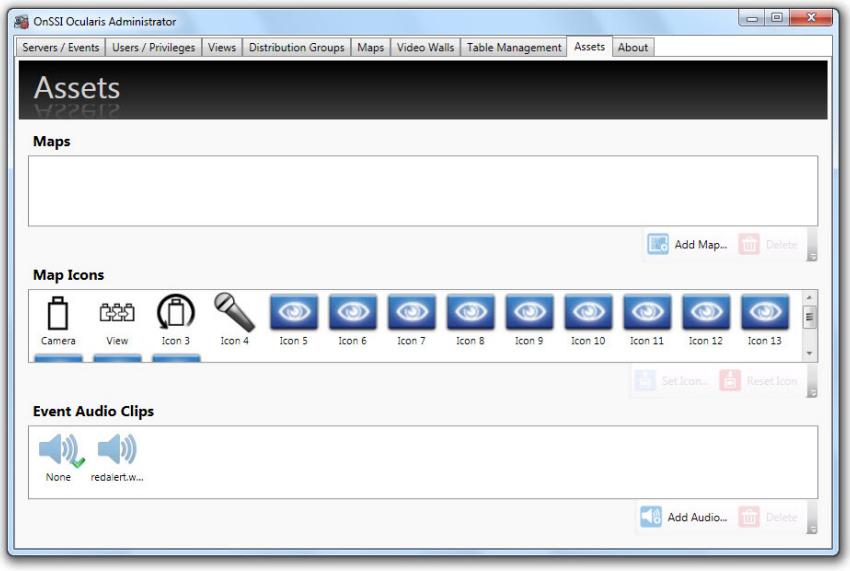


Figure 99 Assets Tab

The Assets Tab is divided into three sections:

1. The upper section displays imported map images.
2. The middle section displays default and imported map icons used for cameras and other items on maps.
3. The lower section displays imported sound files.

Maps

This area houses the navigation maps available for use within the Ocularis Maps feature. Navigation maps can be any descriptive image of the surveillance installation – geographical maps, CAD drawings, aerial photographs, architectural plans, etc. Image file types supported are: .jpg, .png, .gif and .bmp. The system supports an unlimited number of maps.

Map Icons

Icons identify items placed on Ocularis Maps. Icons can be any imported .png image file. Typically, icon images are of IP cameras. The first icon on the left is reserved for the default display when a camera is placed on a map. There is also a default icon for when a view is placed on a map.

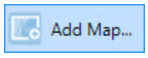
Administrators import maps and icons here in the **Assets** tab first and then continue with map configuration in the **Maps** tab.

Event Audio Clips

Audio files placed here may be used by the administrator to configure the sound played when an event occurs. The default sound is set on the Ocularis Base and is identified by the green checkmark. The default "sound" may be **None,** which therefore indicates no sound during alert notification. The audio file type supported is: .wav.

Maps

To Add a Map to the Assets Tab

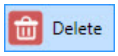
1. In the **Assets** Tab, click the **Add Map** button. 

2. Browse for the image file and select it.
3. Click **Open**.

A thumbnail image of the map appears in the *Maps* area of the Assets Tab. Images are displayed in alphabetical order of the filename.

To Delete a Map from the Assets Tab

Use the following procedure to remove a map image from the Ocularis database. This will not delete the image file from the source location.

1. In the **Assets** Tab, select the map to be removed. You may use the [**SHIFT**] or [**CTRL**] function keys to select multiple files.
2. Click the **Delete** button. 

   An "*Are you sure you want to delete*…?" pop-up window appears.
3. Click **Yes** to remove the map(s).

Map Icons

To Import or Modify a Map Icon

Use the following procedure to set or replace an icon. Icon 1 is the default icon used when creating new items on a map so you may want to leave this icon as the default. Icon 2 is the default icon used for views.

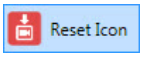
1. In the **Assets** Tab, select the icon to be set.
2. Click the **Set Icon** button.

3. Browse to the image file and select it.
4. Click **Open**.

The icon is displayed in the *Icons* section of the Assets Tab.

To Remove a Map Icon

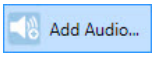
Use the following procedure to remove an imported icon image and reset it to the default.

1. In the **Assets** Tab, select the icon to be changed. You may use the [**SHIFT**] or [**CTRL**] function keys to select multiple icons.
2. Click the **Reset icon** button. 

The icon(s) should be reset.

Event Audio Clips

To Add An Audio File to the Assets Tab

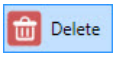
1. In the **Assets** Tab, click the **Add Audio** button. 

2. Browse for the sound file and select it. The maximum size of the .wav file is 4 MB.
3. Click **Open**.

An image with the name of the sound file appears in the *Audios* area of the Assets Tab. Sound files are displayed in alphabetical order of the filename.

To Delete An Audio File from the Assets Tab

Use the following procedure to remove a sound file from *Ocularis Administrator*. This will not delete the file from the source location.

1. In the **Assets** Tab, select the sound file to be removed.
2. Click the **Delete** button. 

   An "*Are you sure you want to delete*…?" pop-up window appears.
3. Click **Yes** to remove the audio file.

To Set or Modify the Default Audio Clip

Ocularis Base is shipped with one default sound file: *redalert.wav*. A blue checkmark symbol indicates the default sound in the **Assets** tab. When an alert notification is configured in the **Servers / Events** Tab, the default sound is assigned to the alert. If the default *Event Audio Clip* is a .wav file, that sound will play when the alert occurs. If the default *Event Audio Clip* is set to 'None', no sound will play when the alert takes place. Administrators can configure sound on an alert by alert basis. A green checkmark indicates that the sound file is already assigned for use to an alert.

1. In the **Assets** Tab, right-click the sound file to be set as the default. Or select 'None' to have no sound as the default
2. Select **Set to Default** in the resulting right-click menu.

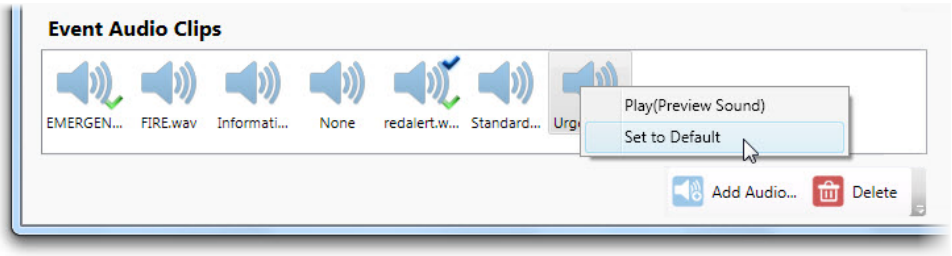


Figure 100 Setting the default Audio Asset

The .wav file now is displayed with the green checkmark to indicate it as the default audio asset.

To Preview An Audio Clip

To preview the sound that a particular .wav file will make when the alert occurs:

1. In the **Assets** Tab, right-click the audio clip to be previewed.
2. Select Play (Preview Sound) in the resulting right-click menu.

The .wav file now is played through the local pc speakers.

Maps Tab

Once maps and icons have been imported in the Assets Tab, they can be configured in the **Maps** Tab.

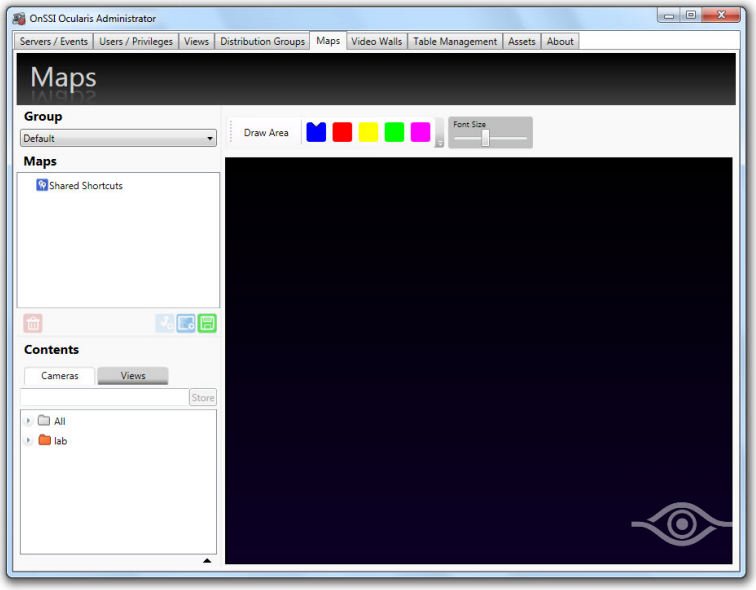


Figure 101 Maps Tab

The left side of the Maps Tab contains elements available for configuring a map and is segmented into a section for **Group** selection, **Maps**, and **Contents** (Cameras and Views). The right side of the Maps Tab is the working area used to display and configure a map.

Maps are configured and organized by user group. Administrators should select the group for which the map should be configured. Maps may be configured for a single user group (“private”) or shared across multiple user groups (“shared”).

> ***Note**:*
> *If you know in advance that a map is to be shared among multiple groups, be sure to configure the map under the Shared Maps group from the beginning. See Sharing Maps on page 116.*

To Add a Map

This procedure assumes that navigation maps have already been imported into the **Assets** Tab and may be used to add a Private or a Shared map. (See *To Add A Map to the Assets Tab* on page 100.)

1. In the **Maps** Tab, select the group from the *Group* drop-down menu for which the map should be available. If you would like the map to be shared between more than one user group, select *Shared Maps* in the drop-down **Group** list.
2. Click the **Add new map** icon.

   The *Select Map* dialog box appears

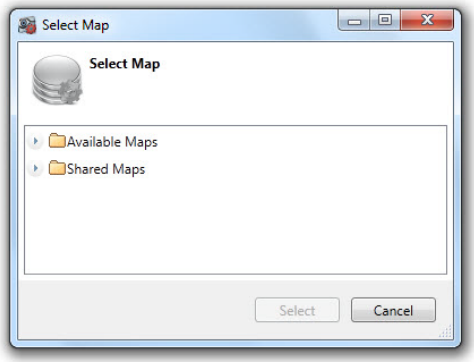


Figure 102 Selecting a Map for a single group (Private)

This pop-up displays the list for *Available Maps* and *Shared Maps*. Available Maps are those which have been imported in the Assets Tab, but not yet assigned to this group or to the Shared Group. Expand Available Maps to see available map images.

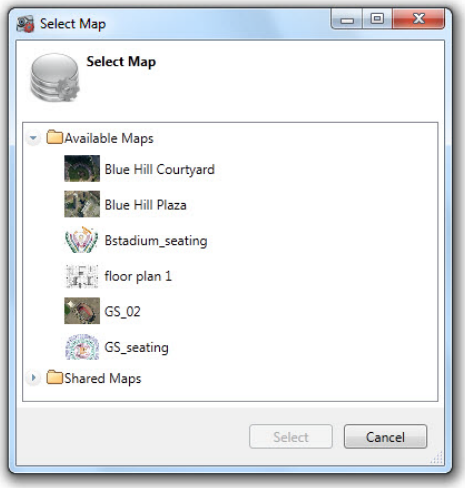


Figure 103 Expand the "Available Maps" folder to choose a map

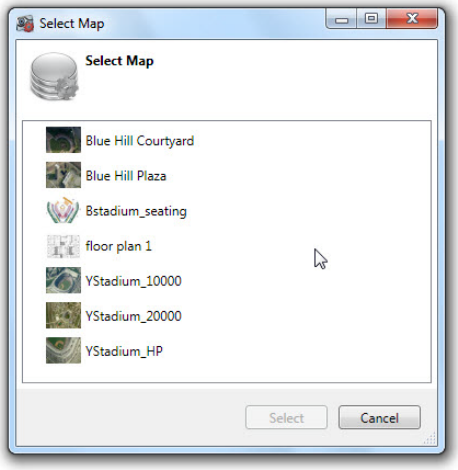


Figure 104 Choosing a Shared Map

When creating a map to be shared by others, the maps displayed here, populated by maps that exist in the **Assets** Tab, are available for selection.

3. Select the map you wish to add.
4. Click **Select**.

The selected map now appears in the Maps list. Expand the node to see its associated Shortcuts and Pins.

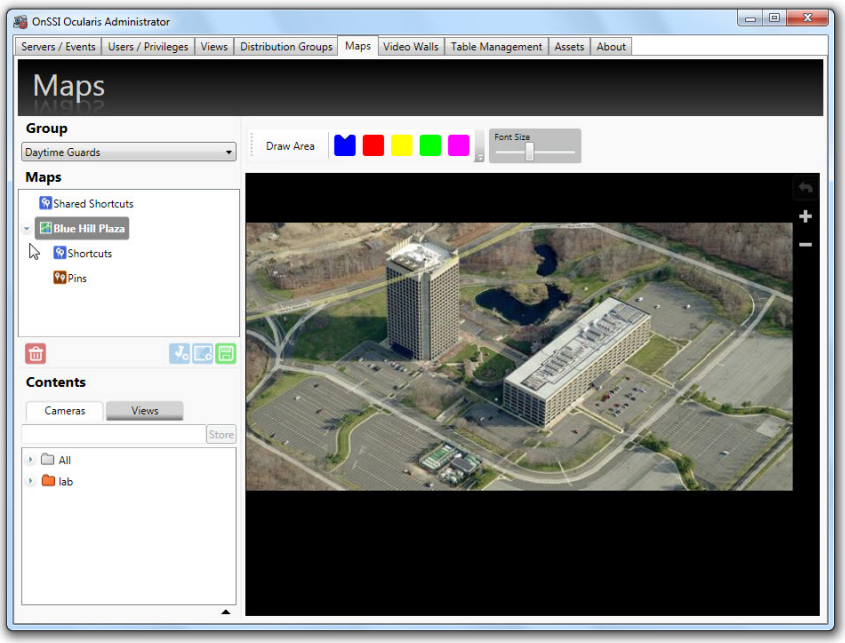


Figure 105 Added Map to Daytime Guards Group

TO DISPLAY A MAP

You need to display a map in order to configure it. This procedure assumes that navigation maps have already been added for the User Group or Shared Maps group in the Maps Tab.

1. Under the desired group, double-click the map name in the Maps list.
2. Reposition the image in the working area by clicking and dragging the map to the desired location.

Once a map is added to a group, a green checkmark icon appears next to the map image in the **Assets** Tab. This helps administrators manage system assets.

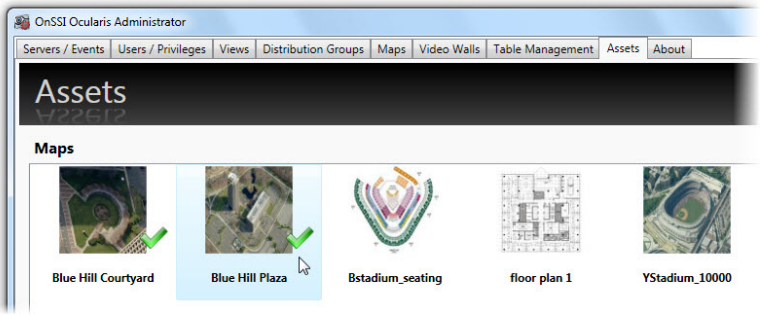


Figure 106 Used Maps in Assets Tab shown with Green Checkmark

In the example shown in Figure 106, the *Blue Hill Courtyard* and *Blue Hill Plaza Map 1* maps have been assigned to a group. The other maps have not been assigned to any group.

TO REMOVE A MAP

1. In the **Maps** Tab, select the map you wish to remove.
2. Click the **Delete Selected Map** icon.

   An "*Are you sure you want to delete this map*?" dialog box appears.
3. Click **Yes** to remove the map.

The map is removed from the group but it is still available to other groups from within Ocularis Administrator.

Working with Maps

Once maps are selected for use in the Maps tab, you can configure it by:

- Add Cameras to A Map
- Add Views to A Map
- Link one map to another Map

Adding Cameras to Maps

Cameras may be added to a map to visually depict its location and field of view. This aids the operator in being able to better understand where it is that the camera is positioned. The accuracy of the location of the camera on the map is subjected to wherever the administrator/map creator decides to place it. On the map, the camera is represented by an icon (which can be modified) and camera name (which is inherited from the recorder). Operators are able to preview the camera feed when viewing the map with Ocularis Client.

TO ADD A CAMERA TO A MAP

1. In the **Maps** tab, display the map to add a camera(s). (see *To Display a Map* on page 105.)
2. Locate the desired camera in the **Contents** area. Click the *Cameras* tab, expand the cameras folder and take advantage of other methods of locating camera such as *Camera Filter* and *Camera Preview*.

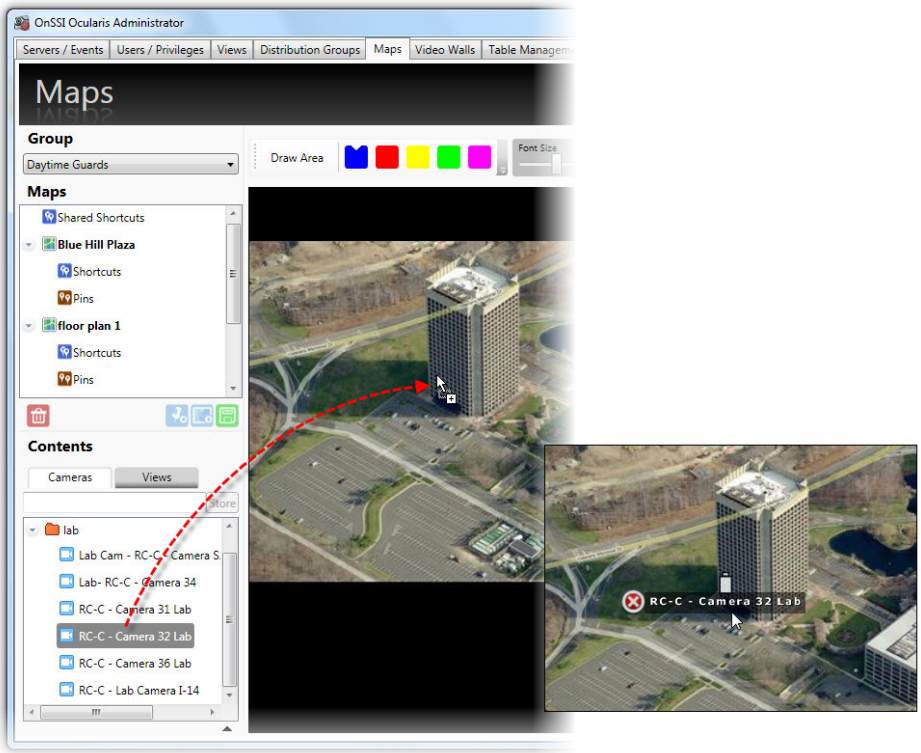


Figure 107 Drag & Drop a camera onto the map

3. Click, drag and drop the camera from the Cameras list to the location on the map.

TO RELOCATE A CAMERA ON A MAP

1. Locate the camera on the map and simply drag and drop the camera to the desired location.

To Remove a Camera From a Map

1. Locate the camera on the map.
2. Click the delete icon next to the camera to delete.

Figure 108 Remove a Camera

Adding Views to Maps

Similar to cameras, views may be added to a map to visually depict multiple cameras. On the map, the view is represented by an icon (which can be modified) and view name. Operators are able to preview the view when viewing the map with Ocularis Client.

To Add a View to a Map

1. In the **Maps** tab, display the map to add the view. (See *To Display a Map* on page 105.)
2. Click the Views tab in the **Contents** list and expand each folder until you locate the desired one.

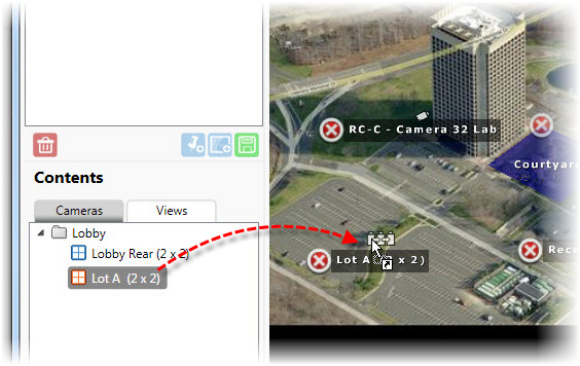


Figure 109 Expanded Views List

3. Click, drag and drop the view from the Views list to the location on the map.

The view will use Icon 2 located in the Assets Tab. You may want to develop your own icon for use specifically for views.

> ***Note**:*
> *Views that contain a Hotspot pane may not be added to a map and will appear grayed out in the Views list. Views that contain a Blank Screen, Push Video or Web page may be added but the pane with these content types will not display any preview images.*

To Change the Appearance of a Map Icon

The first image shown in the Icons section in the Assets tab is the default icon used when adding cameras to maps. The second icon is the default used for views. You may customize the icons for each camera to signify a camera model or type or any designation you so choose. (See *To Import or Modify* an Icon on page 100).

1. Locate the camera icon or view icon on the map you wish to change.
2. Right-click the icon.
3. The icons from the **Assets** tab appear. Click the desired icon.

TO MODIFY THE FONT SIZE OF MAP ICONS

The descriptions associated with icons on a map come from either the camera name on the recorder or the view name in the Views tab. The size of the fonts used may be made larger or smaller.

1. Open the desired map in the **Maps** tab.
2. Drag the Font Size slider button left or right to make the font size smaller or larger.

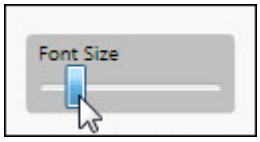


Figure 110 Change font size with slider

TO RESIZE A MAP ICON

1. Locate the camera or view icon on the map you wish to change.
2. Hold the [**SHIFT**] key and position the mouse over the icon until you see a set of 4 arrows.
3. Click and drag the mouse in a vertical direction up and down to make the icon larger or smaller.
4. Release the mouse when done.

Figure 111 Resize a camera icon

TO ROTATE A MAP ICON

1. Locate the camera or view icon on the map you wish to change.
2. Hold the [**CTRL**] key and position the mouse over the icon until you see a curved arrow.
3. Click and drag the mouse in a vertical direction up and down to rotate the icon.
4. Release the mouse when done.

Figure 112 Rotate a camera icon

TO ZOOM A MAP

1. Display the map in the working area of the **Maps** tab.
2. Zoom in and out using either the:
    - Scroll wheel of the mouse
    - Zoom In or Zoom Out icon

Linking Maps

Linking maps allows you to easily navigate from map to map and back again. Links to maps can be embedded within a map or displayed as floating links within the map display.

- To Embed a Link in a Map
- To Display A Floating Map Link

Shortcuts and Pins

A *Shortcut* is a link that appears on one map that, when clicked, will navigate the screen to another map. The shortcut inherits its name from the *pin* used. A *Pin*, is a shortcut name given to a location on a particular map and is created by the administrator. The pin sets the destination map as well as its horizontal position, vertical position and zoom level.

Prior to creating an embedded or floating link, you must first set the pin(s) on the map(s).

TO SET A MAP PIN

1. In the **Maps** Tab, with the desired group selected, open the *destination* map or the map to which you would like be linked. This is the map that must include the pin(s).
2. Position the map on the screen and zoom in or out so that the map is positioned in the location you wish it to be displayed when it is brought up by the link.
3. Click the **Add New Pin** icon.
4. In the resulting **Enter Pin Name** dialog box, enter a descriptive name for this pin. Keep in mind that the pin name is going to be displayed on the map on either a clickable link area or a floating map link. It is recommended that pin names be kept as concise as possible.
5. Click **OK**.

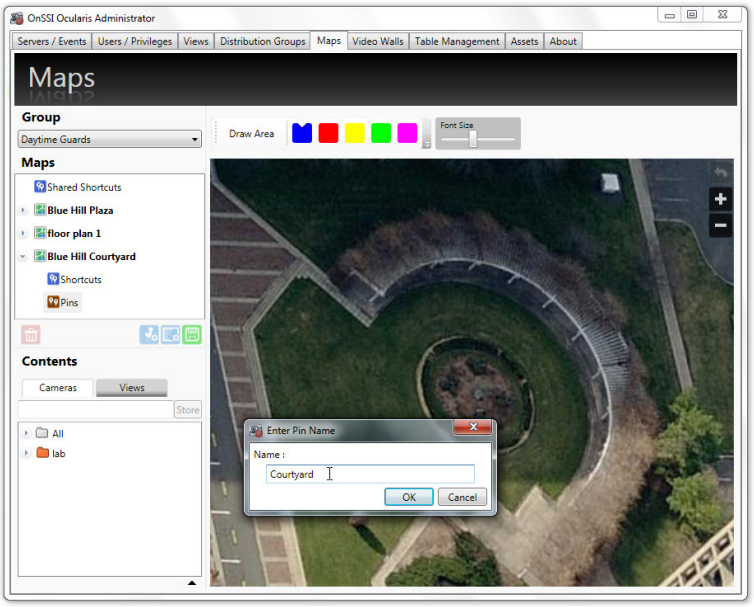


Figure 113 Courtyard map with corresponding pin

6. Repeat steps 1-5 above to add additional pins to a map.

To Embed a Link in a Map

1. In the **Maps** Tab, with the desired group selected, be sure to have already set the pins on the destination map. See *To Set a Map Pin* on page 111.
2. Display the map on which you would like to place the embedded link.
3. You need to draw an area or zone where when clicked, will open up the linked map. Click the **Draw Area** button.

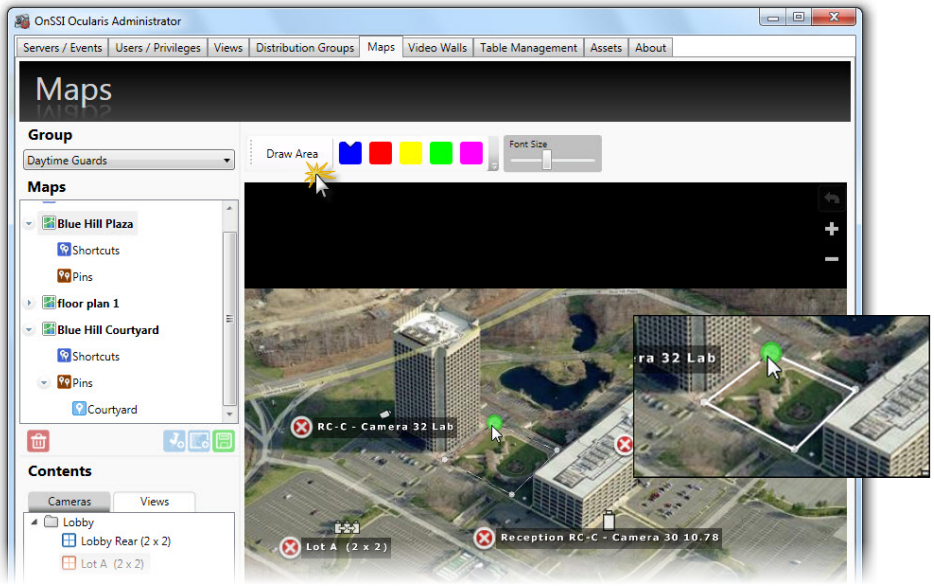


Figure 114 Draw Link Area

4. Use the mouse to draw a polygonal shape on the map which will link to the previous map. Click, release and drag with the right-button and when you get to a corner, click the right-button. Repeat this process for each leg of the shape. When you return to the starting point (“pencil”), the shape outline turns white. Click the right mouse button and releasing the mouse establishes the shape.

   The shape will appear shaded in color and be labeled “unnamed”.

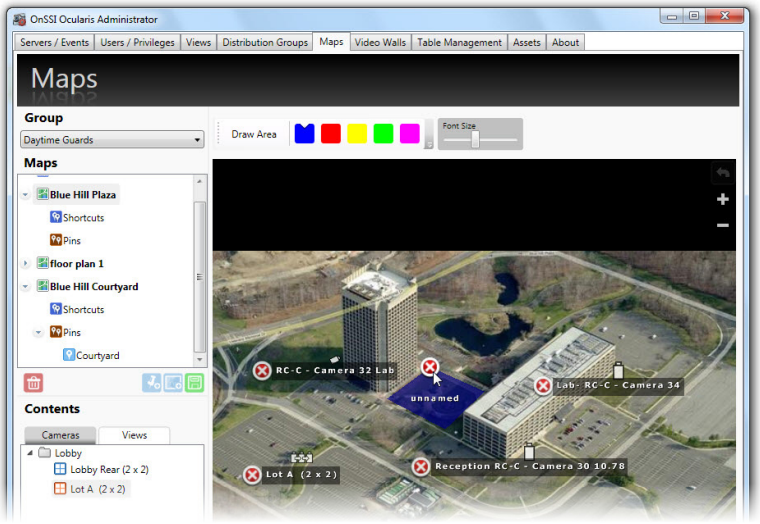


Figure 115 Link Area unnamed and unassigned

5. Click and drag a pin created earlier onto the unnamed shaded area.

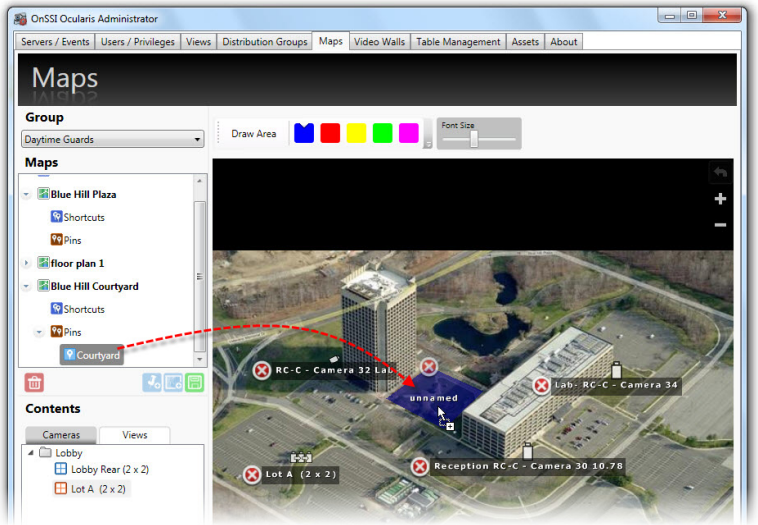


Figure 116 Pin Name Link

The area name will change to display the pin name.

Figure 117 Link area inherits pin name

6. Click the pin area to be brought to the linked map.

To Return to Original Map From a Linked Map

Once you have navigated to a map via a link, you may return to the original map by either:

- Creating another pin to the original map using steps 1- 5 in the above section.
- Click the **Go Back** icon.

To Modify the Color of the Link Area

The default color for a map link is blue. If you want, you may change the color for each area from the available palette of colors.

1. Display the map with the link area.
2. Drag and drop the desired color from the color palette to the link area.

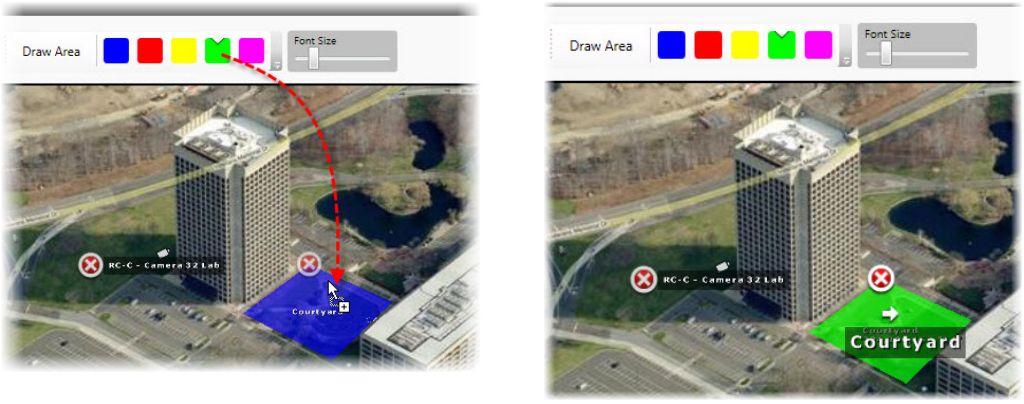


Figure 118 Drag & drop color to modify link area

To Display A Floating Map Link (Shortcut)

Floating map links or Shortcuts are easy to assign to multiple maps and appear on the Ocularis map when it is displayed in *Ocularis Client*. They are particularly useful in navigating very large maps. These links may appear on a single map or all maps for the selected group.

In the Maps list, beneath each map, is a node for Shortcuts. These shortcuts are similar to link areas in that, when click in *Ocularis Client*, they will navigate the screen to the map with the associated pin.

Floating Map links/shortcuts can be assigned to a map on an individual basis or to all maps of the group. The map on which the floating link appears can be considered the ‘source’ map and the map which is navigated to when the link is clicked can be considered the ‘destination’ map.

1. In the **Maps** Tab, with the desired group selected, be sure to have already set the pins on the destination map(s). See *To Set a Map Pin* on page 111. In the Maps list, expand the destination map node displaying the pin name.

2. Determine the source map on which you would like the floating links to appear. Expand the source map node to expose **Shortcuts** and **Pins**.

3. Drag and drop the pin from the destination map to the corresponding pin node of the source map.

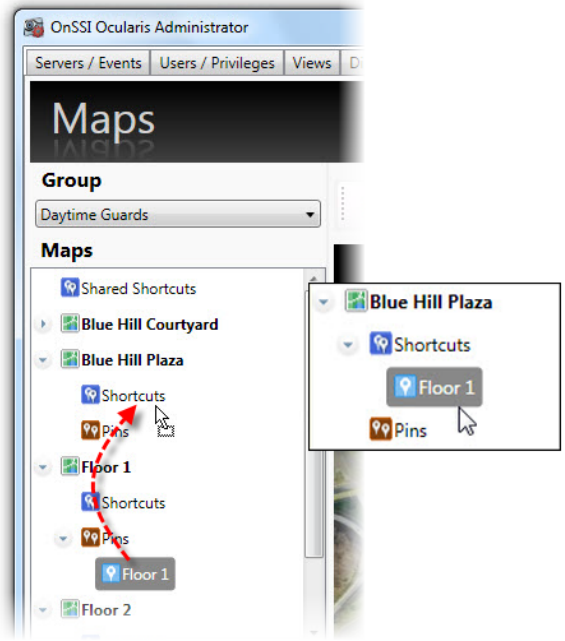


Figure 119 Drag and drop Map Pin

The map appears in the map's **Shortcuts** list.

4. Repeat for each map pin you wish to add.

5. Click the **Save** icon to save the map configuration.

If you wish to assign the pin as a shortcut for all maps of the selected group in one step, drag the pin to the **Shared Shortcuts** node. This shortcut will appear on all of the group's maps.

For example:

The Blue Hill Plaza map has three Shortcuts configured in *Ocularis Administrator* **Maps** tab as shown in Figure 120.

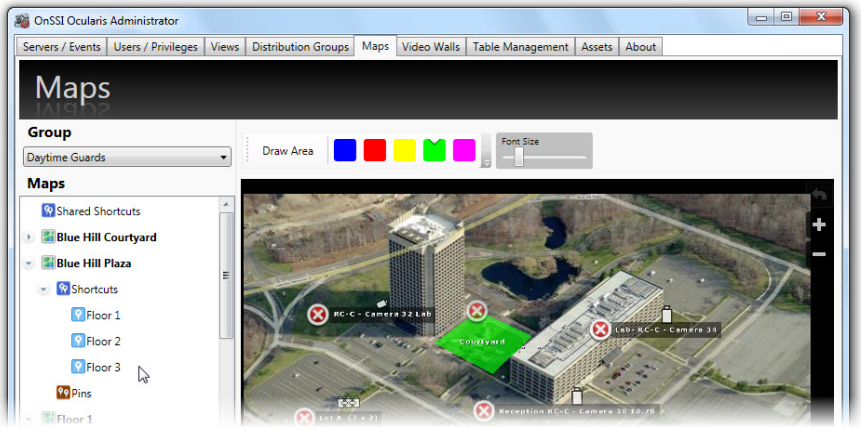


Figure 120 Example with three Shortcuts

In *Ocularis Client*, the shortcuts will appear as shown in Figure 121.

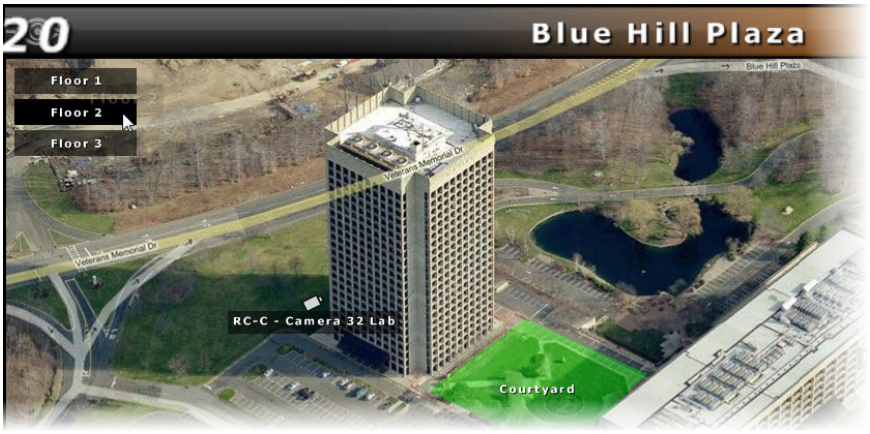


Figure 121 Map with three floating map shortcuts

Sharing Maps

Creating a map that is to be shared among multiple user groups is the same process as creating one for a single user group. See *To Add a Map* on page 103 as well as the preceding pages for configuring maps. The difference with shared maps is where the map is created.

To Share a Map

1. In the **Maps** tab, select *Shared Maps* from the **Groups** drop-down list.
2. Add a map(s) to the Shared Maps group. (See Figure 104 on page 104.)
3. Add cameras and views to the map as needed.
4. Add navigation links to the maps as needed.
5. Once the shared map is configured as desired, click the **Save Layout** icon.

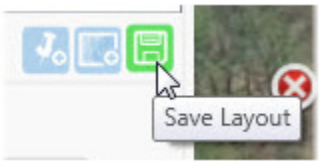


Figure 122 Save Layout icon

6. Select the user group from the **Groups** drop-down list that you would like to have access to this map.
7. Click the **Add New Map** icon.
8. Expand the Shared Maps folder from the Select Map pop-up to see the list of available Shared Maps.

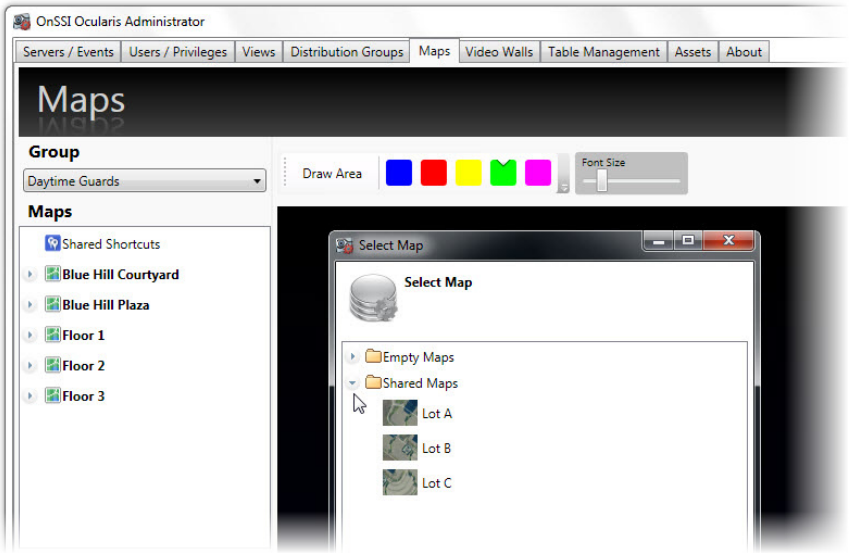


Figure 123 Add from Shared Maps folder to share a map

9. Select the desired map from the list shown and click **Select**.
10. Repeat for each shared map you would like to be assigned to this group.

When you view a shared map from the user group's perspective, a padlock icon appears on the map name in the maps list, indicating that the map is a shared map and may not be edited from the user group location.

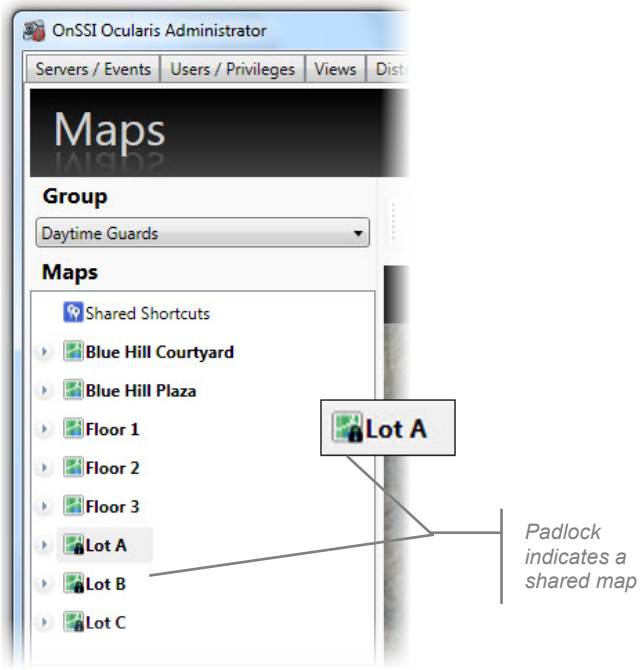


Figure 124 Padlock icon indicates a shared map

Like shared views, shared maps may only be modified from the Shared Maps group. Likewise, new changes to the shared map will be reflected in each groups' view of the map.

***Note**:*
Cameras displayed on a shared map are controlled via the user group's privileges to that camera in the Users/Privileges tab. If a user group does not have permission to view a camera or view, it will not appear on their view of the shared map.

Event Management

Ocularis facilitates displaying, investigating and shared handling of events received from:

- A recorder's native video motion detection (VMD) component
- Attached Devices
- Integrated Video Content Analytics
- Third party access control and security systems

Administrators determine which events to which a user should be alerted. Ocularis events maintain the following features:

- ⇨ Incoming events appear in the *Alerts Manager* in the *Ocularis Client*.
- ⇨ Video walls and Views containing a Blank Screen will display video from configured events.
- ⇨ Alert notifications may be designated with low, medium or high priority. Events with high priority will display on an *Ocularis Client* blank screen pane until a user "handles" the event. Medium or low priority alerts display for a designated time period.
- ⇨ Alerts appear in the order of occurrence

Each alert is accompanied by relevant metadata. Typically this includes the camera name that captured the event, time, date and type of event. The type of event is specified in generic terms (e.g. 'VMD Event') or, in the case of video content analytics or access control-generated events, by the analytics rule that triggered the event (e.g. "Stalled Vehicle on Shoulder').

Multiple authorized operators can share the investigation and handling of events through the dynamically-updated *Alerts Manager* in *Ocularis Client*. Once an event is 'handled', it is removed from the *Alerts Manager*. In this case, subsequent investigation is possible only through *Handled Alerts* in the *Ocularis Client*.

> ***Note**:*
> *Camera events are supported with Ocularis ES, Ocularis LS, Ocularis CS and Ocularis IS.*
>
> *In order to use camera events with Ocularis Base, an event proxy must first be installed. See the Ocularis Installation & Licensing Guide for instructions on installation and configuration of supported event proxies.*

Event Configuration

Camera related events which may be monitored include (but are not limited to):

- Motion in the camera field of view
- Camera is enabled
- Camera is disabled
- Camera is not responding
- Video Signal change (rise or fall)
- Audio Signal change (rise or fall)
- Tampering

Software specific events include:

- VMD Event

Third party events include:

- Analytic Event
- Generic / Data Link Event

To instruct Ocularis which events you wish you monitor and create event associations, see Events Pane on page 34.

Quick Reference – EVENTS

The following steps are necessary in order for events to work properly with Ocularis.

EVENT CONFIGURATION WITH OCULARIS BASE

Follow these basic instructions to insure event configuration is done properly.

1. In the *Ocularis Administrator* **Server / Events** tab, if applicable, add the recorder which contain the events you wish to monitor.
2. Locate the associated event proxy in the *Events* pane.
3. In the *Ocularis Administrator* **Server / Events** tab, drag cameras listed in the *Servers* pane to the events you want to enable in the *Events* pane. (see To Create an Event Rule (To Associate Camera Video with Events) on page 37).
4. If desired, change the priority of the alert by highlighting the event and clicking the **Properties** button. (see To Modify the Priority of an Event on page 39).
5. If desired, modify the sound played when the event occurs. (see To Modify the Audio of an Event on page 41).
6. In the *Ocularis Administrator* **Users / Privileges** tab, make sure the appropriate user has privileges to the device. (see Assign Devices To A User Group on page 64).
7. In the *Ocularis Administrator* **Distribution Groups** tab, be sure that the user is assigned to a distribution group which has corresponding events assigned in the group's events and that the weekly and holiday schedules are set appropriately. (see Distribution Groups on page 126).
8. The OnSSI Event Coordinator service must be running on the Ocularis Base machine. (See The OnSSI Event Coordinator on page 145).
9. When a configured event occurs, it will be listed in the *Alert Manager* of the *Ocularis Client* and in a blank screen pane (if one is visible).

Event Handling

As events are triggered and alerts are displayed in the *Ocularis Client*, the operator has the opportunity to handle or ignore the alert.

When a user handles an event through the *Ocularis Client*, it can be assigned a *Classification*, a *Tag* or *Case File*. These provide the operator with a means of organizing the alert. These organizational parameters are configured in the **Table Management** tab of the *Ocularis Administrator*. For information on handling events in Ocularis Client, see the *Ocularis Client User Manual*.

Table Management Tab

The following tasks are available on the **Table Management** Tab:

- Configure Classifications
- Configure Tags
- Configure Cases

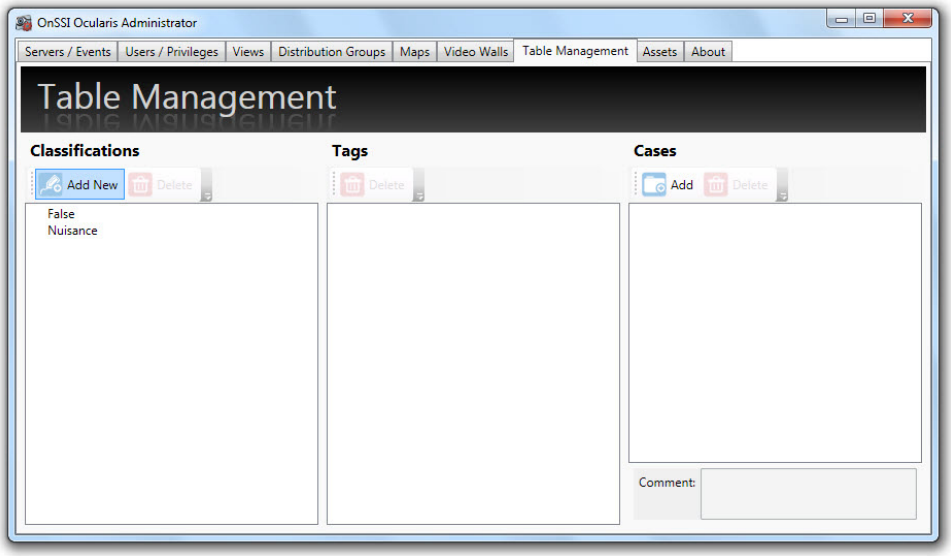


Figure 125 Table Management Tab

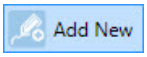
The **Table Management** tab is divided into 3 vertical panes: *Classifications*, *Tags*, and *Cases*.

Configure Classifications

When operators handle events or create a bookmark in the *Ocularis Client*, the event or bookmark may be categorized into predefined classes as defined by the system administrator. The default classifications are:

- False
- Nuisance

TO CREATE A NEW CLASSIFICATION

1. In the **Table Management** tab, click the **Add New** button in the **Classifications** pane. 

   A 'New Classification' field is inserted into the Classifications list.

2. Double-click this entry to modify the label.
3. Press **[ENTER]**.

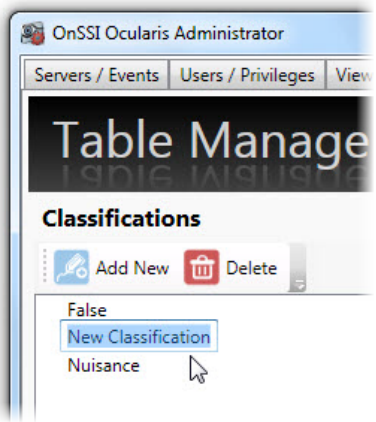


Figure 126 Add a new Classification

TO MODIFY A CLASSIFICATION

1. In the **Table Management** tab, double-click the classification you wish to modify.

   The field should become editable.

2. Type in text changes as desired.
3. Press **[ENTER]**.

> ***Note**:*
> *Modifying the name of a classification is global. Therefore, If you modify the name of a classification that has already been used in a bookmark or handled event, it will also change in that bookmark or handled event.*

TO DELETE A CLASSIFICATION

1. In the **Table Management** tab, select the classification you wish to delete.
2. Click the **Delete** button in the **Classifications** pane.

3. An "*Are you sure that you want to delete this classification…*" pop-up appears. Click **Yes** to delete the classification.

> ***Note**:*
> *Classifications which have been used in a bookmark or handled event may not be deleted.*

> ***Note**:*
> *Classifications may also be created on the fly from the Ocularis Client as an operator is handling the event. Classifications, however, may only be modified or deleted through the Ocularis Administrator.*

Configure Tags

When operators handle events or create bookmarks in the *Ocularis Client*, he or she may assign a tag or keyword to the event. Administrators may modify or delete tags entered by operators in the *Ocularis Administrator* **Table Management** tab.

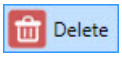
TO MODIFY A TAG

1. In the **Table Management** tab, double-click the tag you wish to modify.

   The field should become editable.
2. Type in text changes as desired.
3. Press **[ENTER]**.

> ***Note**:*
> *Modifying the name of a tag is global. Therefore, If you modify the name of a tag that has already been used in a bookmark or handled event, it will also change in that bookmark or handled event.*

TO DELETE A TAG

1. In the **Table Management** tab, select the tag you wish to delete.
2. Click the **Delete** button in the **Tags** pane. 

3. An "*Are you sure that you want to delete this tag…*" pop-up appears. Click **Yes** to delete the tag.

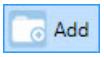
> ***Note**:*
> *Tags which have been used in a bookmark or handled event may not be deleted.*

***Note**:*
Tags are created on the fly from the Ocularis Client as an operator is handling an event or creating a bookmark. Tags, however, may only be modified or deleted through the Ocularis Administrator.

Configure Cases

When operators handle events or create bookmarks in the *Ocularis Client*, the event or bookmark may be assigned to an incident case. The use of an incidence case file is optional. Case names can be created in *Ocularis Administrator* by the system administrator or on the fly as an operator is handling a case.

To Create A New Case

1. In the **Table Management** tab, click the **Add** button in the **Cases** pane. 

   A 'New Case' entry is inserted into the Cases list.

2. Double-click this entry and type in a descriptive name for the Case.
3. Press **[ENTER]**.

To Modify A Case

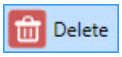
1. In the **Table Management** tab, double-click the case you wish to modify.

   The field should become editable.

2. Type in text changes as desired.
3. Press **[ENTER]**.

***Note**:*
Modifying the name of a case is global. Therefore, If you modify the name of a case that has already been used in a bookmark or handled event, it will also change in that bookmark or handled event.

To Delete A Case

1. In the **Table Management** tab, select the case you wish to delete.
2. Click the **Delete** button in the **Cases** pane. 

3. An "*Are you sure that you want to delete this case*…" pop-up appears. Click **Yes** to delete the case.

***Note**:*
Cases which have been used in a bookmark or handled event may not be deleted.

***Note**:*
Cases may also be created on the fly from the Ocularis Client as an operator is handling an event. Cases, however, may only be modified or deleted through the Ocularis Administrator.

Distribution Groups Tab

In the **Servers / Events** Tab, system administrators configure the events which should be monitored on the entire system. The **Distribution Groups** Tab provides system administrators with the ability to configure the distribution of alert notifications for system events. The system administrator determines which alerts to group together, to whom alert notifications should be distributed, if any actions should occur upon event trigger and when alerts should be received. A user must be assigned to a distribution group in order for that user to receive alerts. Additionally, for alerts to be visible on a video wall blank screen s

Distribution Groups are also designed to filter the myriad of alerts and “distribute” them to only those users who really need to see them. As an example, you may want to alert the weekend lobby security guard of only the alerts generated in or near the lobby during weekend hours. There may be many distribution groups configured depending on the number and complexity of events being monitored.

The **Distribution Group** tab is divided into two panes: on the left is the list of existing Distribution Groups and on the right is the detail for a selected group or item. Before a user can view events in the Alerts Manager in *Ocularis Client*, the user must be assigned appropriate permissions in this tab.

TO CREATE A DISTRIBUTION GROUP

1. In the **Distribution Groups** Tab, click the **New Group** button.

   A ‘New Distribution Group’ entry is inserted into the Distribution Groups list.

2. Double-click the entry and type in a descriptive name for the Distribution Group.

3. Press **[ENTER]**.

The new group appears in the **Distribution Groups** list.

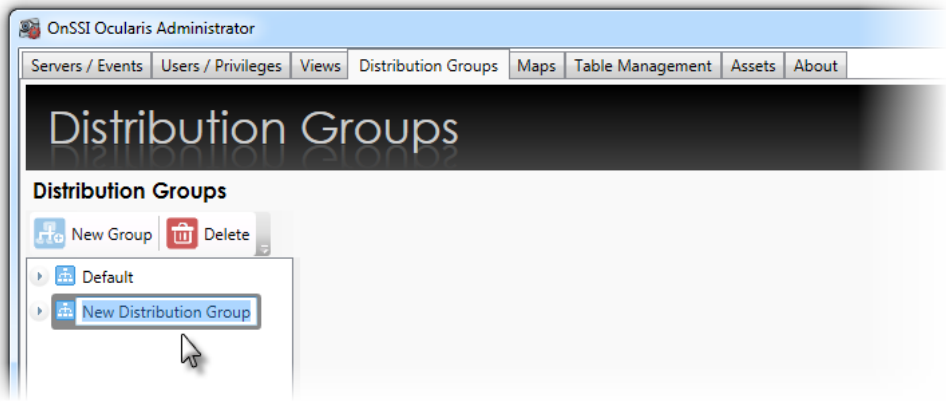


Figure 127 Distribution Group Tab

TO MODIFY A DISTRIBUTION GROUP

1. In the **Distribution Groups** Tab, double-click the Distribution Group you wish to rename.

2. The text becomes highlighted. Make the required change and press **[ENTER]**.

TO DELETE A DISTRIBUTION GROUP

1. In the **Distribution Groups** Tab, select the Distribution Group you wish to delete.
2. Click the **Delete** button.
3. In the "*Are you sure you want to delete the distribution group…*" pop-up, click **Yes** to delete the group.

Distribution Groups

There are six (6) parameters to configure for each Distribution Group:

- Events
- Users
- Actions
- Video Walls
- Weekly Schedule
- Holiday Schedule

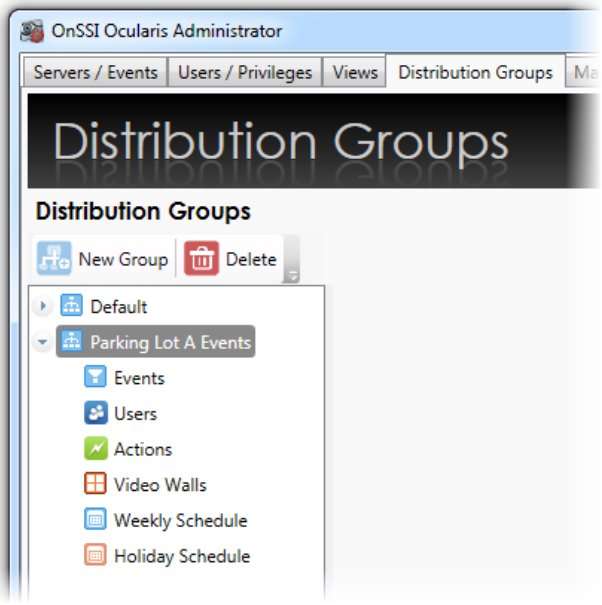


Figure 128 Distribution Group parameters

Events

Formerly labeled ‘Filter’, the Events item is used to identify the events to be configured in this group.

To Assign Events to a Distribution Group

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Events** item for the group you wish to configure.

   The tab updates and displays two panes: **All Available Events** and **Enabled Events in this Distribution Group**.

2. Drag & drop an event from the **All Events** list on the left to the **Users in Distribution Group** pane on the right.

   - You may move one event at a time or the entire hierarchical group of events.
   - You may move composite events, generic events or any event listed in the All Events pane.

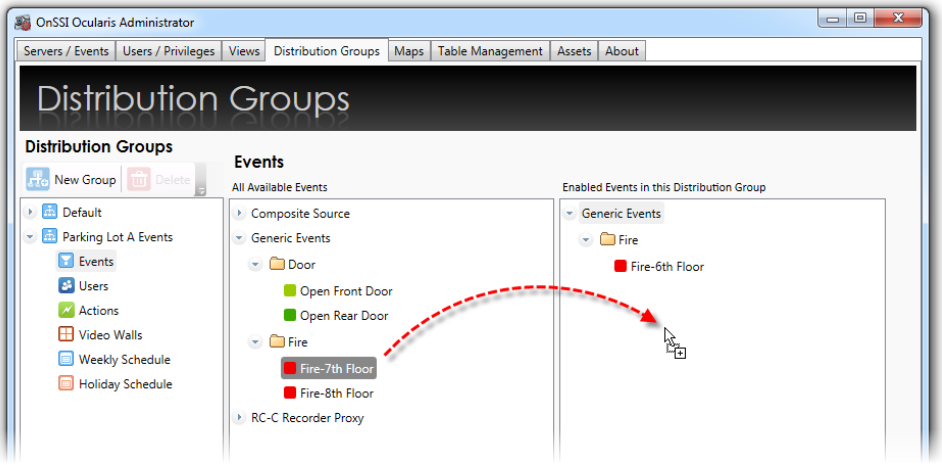


Figure 129 Assigning Events to a Distribution Group

> ***Note:*** *When new events are added/configured in the Servers / Events tab, you must return to the Distribution Groups tab and assign the events to a group in order for users to be alerted to the event(s).*

To Modify Event Assignments within a Distribution Group

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Events** parameter for the group you wish to modify.
2. Modify event assignments by dragging & dropping an event from the **Enabled Events** list on the right to the **All Available Events** pane on the left to remove an event assignment.
3. Drag a new event from the **All Available Events** pane to the **Enabled Events** list.

You may move one event at a time or the entire hierarchical group of events.

To Delete Events from a Distribution Group

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Events** item for the group you wish to modify.

2. Remove event assignments by dragging & dropping an event from the **Enabled Events** list to the **All Available Events** pane to remove an event assignment.

Users

Once the events for the group have been determined, the user account for distribution may be assigned next.

To Assign a User to a Distribution Group

1. In the **Distribution Groups** Tab, expand a group and highlight the **Users** parameter for the group you wish to configure.

   The tab updates and displays two panes: **All Users** and **Users in Distribution Group**.

2. In the **All Users** pane, expand the user group which contains the user you want to assign.
3. Drag & drop the user name from the **All Users** list on the left to the **Users in Distribution Group** pane on the right.

   - You may only move one user at a time
   - Users from different user groups may be assigned to the same distribution group
   - The same user may be assigned to multiple distribution groups

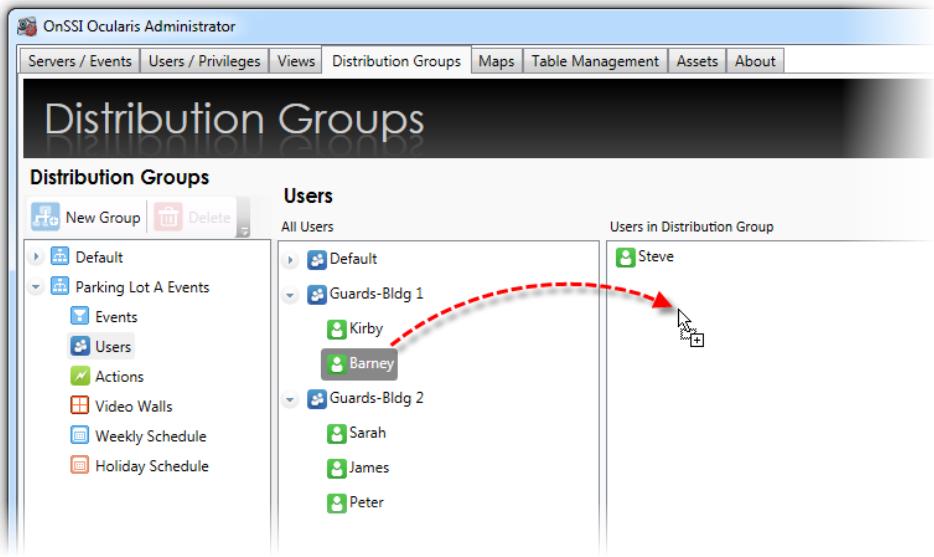


Figure 130 Drag & Drop to Assign Users to Distribution Groups

***Note on Group Administrators**: Users with the* Group Administrator *privilege may create Distribution Groups and include only those users within their User Group. Group Administrators may have users in their Distribution Group that are not part of their User Group because they were added by the **admin** user. In this case, Group Administrators do not have permission to edit or remove these users as their names will be grayed out.*

TO UNASSIGN A USER FROM A DISTRIBUTION GROUP

1. In the **Distribution Groups** Tab, expand the group and highlight the **Users** parameter for the user you wish to remove.
2. Drag & drop the user name from the **Users in Distribution Group** list on the right to the **All Users** pane on the left.

Actions

A resulting action may be assigned to take place should an event occur. These actions, (Move to Preset, Send Email, Send HTTP Request, and Send TCP/UDP Data Packet) are configured in the **Servers / Event**s tab but assigned to events in the **Distribution Groups** tab.

TO ASSIGN AN ACTION TO A DISTRIBUTION GROUP

1. In the **Distribution Groups** Tab, expand a group and highlight the **Actions** item for the group you wish to configure.
2. In the **All Actions** pane, expand the Action which contains the item you want to assign.
3. Drag & drop the Action item from the **All Actions** list on the left to the **Actions in Distribution Group** pane on the right. You can drag & drop all action items by dragging the Action top level item. ***In most cases, you probably do not want to do this!***

TO UNASSIGN AN ACTION FROM A DISTRIBUTION GROUP

1. In the **Distribution Groups** Tab, expand the group and highlight the **Actions** parameter.
2. Drag & drop the Action item from the **Actions in Distribution Group** list on the right to the **All Actions** pane on the left.

Video Walls

For events to be posted to a video wall in a blank screen and in sequence, the video wall must be included in the alert distribution group. Remote video walls are supported with Ocularis ES, Ocularis LS, Ocularis CS and Ocularis IS.

TO ASSIGN A VIDEO WALL TO A DISTRIBUTION GROUP

1. In the **Distribution Groups** Tab, expand a group and highlight the **Video Walls** parameter for the group you wish to configure.

The tab updates and displays two panes: **All Video Walls** and **Video Walls in Distribution Group**.

2. In the **All Video Walls** pane, drag & drop the video wall from the **All Video Walls** list on the left to the **Video Walls in Distribution Group** pane on the right. Video walls are created in the **Users / Privileges** tab so if you need to create a new one, do so in that tab.

You may assign multiple video walls to a distribution group.

Weekly Schedule

Schedules for Distributions Groups can be set up to allow alert notification only during specific dates and times. This decreases the amount of alerts shown to a given user, making managing alerts an easier task.

By default, the Weekly Schedule is set to be on 24/7, seven days a week.

> ***Note:*** *These schedules can be overridden in the Ocularis Client if the user account has been given the Event Filtering privilege in the Users/Privileges tab.*

TO SET A WEEKLY SCHEDULE

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Weekly Schedule** parameter for the group whose weekly schedule you wish to set.

   A **Weekly Schedule** appears in the details pane.

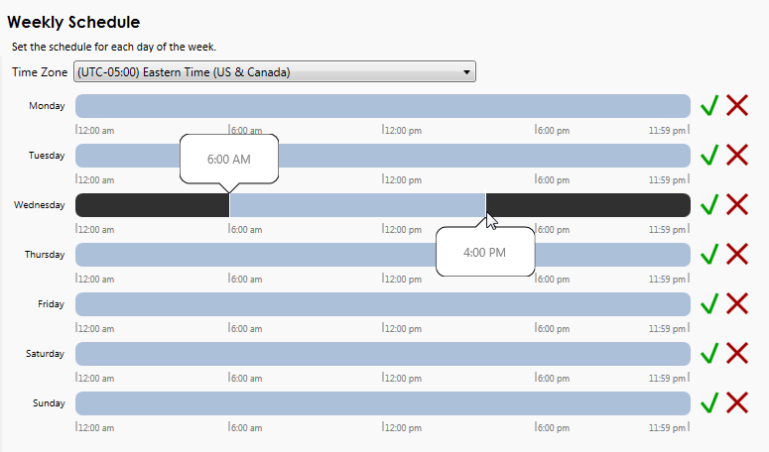


Figure 131 Setting a Weekly Schedule

> ***Tip****: If you position the mouse over the timescale, a balloon appears displaying the Start and End time on the timescale.*

2. At the top of the calendar, a time zone drop-down list is available. Select the time zone for the Distribution Group. Alerts will be active for the members of this group during the time period of the time zone selected.

> ***Note:*** *Time zones selected here apply to the distribution group, regardless of the users in it. For instance: if the Distribution Group has a time zone assignment for Pacific Time and an alert window is set for 9:00 a.m. to 5:00 p.m., the alert would be distributed to the designated members of the group during this time. A member of this group who happens to be located in the Eastern Time zone, would therefore, receive alerts locally between 12:00 p.m. – 8:00 p.m.*

The time zone set for the group's Weekly Schedule is shared with the time zone for its Holiday Schedule.

3. For each day of the week, click and drag to set the time schedule. Click the icon to clear the daily schedule.
4. When you release the mouse, after clicking and dragging to designate a time period, the *Time Range* pop-up appears with the **Start Time** and **End Time** displayed.

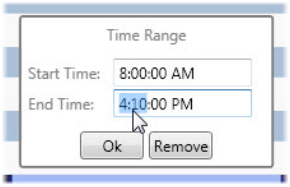


Figure 132 Time Range Pop-Up

5. Make changes manually as necessary. Click **Ok** to save the *Time Range* settings.
6. Repeat for each day of the week.

You may set multiple time ranges within a given day.

TO MODIFY A WEEKLY SCHEDULE

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Weekly Schedule** parameter for the group whose weekly schedule you wish to modify.

   The **Weekly Schedule** appears in the details pane.
2. Click on a Time Range you wish to modify.

   The **Time Range** pop-up appears as shown in Figure 132.
3. Modify the **Start Time** and / or **End Time** as needed.
4. Click **Ok** to save the *Time Range* settings.
5. Repeat steps 1-4 for each day of the week you wish to modify.

TO CLEAR A WEEKLY SCHEDULE

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Weekly Schedule** parameter for the group whose weekly schedule you wish to delete.

   The **Weekly Schedule** appears in the details pane.
2. Click on the **Clear Schedule** icon next to the day of the week you wish to clear.

Figure 133 Clear a Weekly Schedule

The schedule for that day has been removed.

Figure 134 Cleared Schedule for Monday

3. Repeat for each day of the week whose schedule you wish to clear.

TO RESET A WEEKLY SCHEDULE

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Weekly Schedule** parameter for the group whose weekly schedule you wish to reset.

   The **Weekly Schedule** appears in the details pane.

2. Click on the **Reset Schedule** icon next to the day of the week you wish to reset.

Figure 135 Reset a Weekly Schedule

The schedule for that day has been reset to the default of 24 hours.

3. Repeat for each day of the week whose schedule you wish to reset.

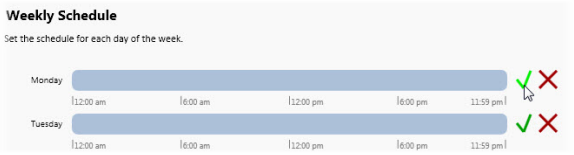


Figure 136 Reset Schedule

Holiday Schedule

Weekly schedules are for general use throughout the year. However, during days when an organization works a limited number of hours or with a limited number of employees, a Holiday Schedule can be followed.

Holiday Schedules are set on a distribution group basis and override any time range set in a Weekly Schedule.

By default, no Holiday Schedule is set and therefore, this task must be done for each Distribution Group. The time zone selected for the Holiday Schedule applies to the Distribution Group as a whole and must be the same time zone used as the Distribution Group's Weekly Schedule.

TO SET A HOLIDAY SCHEDULE

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Holiday Schedule** parameter for the group whose Holiday Schedule you wish to set.

   The details pane displays a Holiday Schedule with a pull-down menu for the year and an **Add New Holiday** icon.

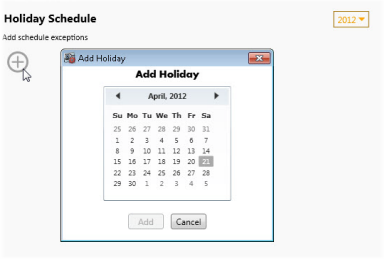


Figure 137 Holiday Schedules

2. Select the year for the holiday from the year drop-down menu.
3. Click the **Add New Holiday** icon.

   An **Add Holiday** pop-up appears displaying a calendar.
4. Navigate to the month and day for the holiday and click the date to select it.
5. Click the **Add** button to add the date to the Holiday Schedule.
6. Once the date is added, the Time Range for the Holiday should be specified. Click and drag along the timescale to select the Start and End times.
7. Repeat steps 1-6 for each Holiday for this Distribution Group.

To Modify a Holiday Schedule

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Holiday Schedule** parameter for the group whose Holiday Schedule you wish to modify.

   The details pane displays the group's Holiday Schedule.

2. To modify a Time Range, click on the range and change the Start Time and / or End Time directly and then click Ok.

3. To Add an additional holiday, click the **Add New Holiday** icon.

4. Navigate to the month and day for the holiday and click the date to select it.

5. Click the **Add** button to add the date to the Holiday Schedule.

6. Once the date is added, the Time Range for the Holiday should be specified. Click and drag along the timescale to select the Start and End times.

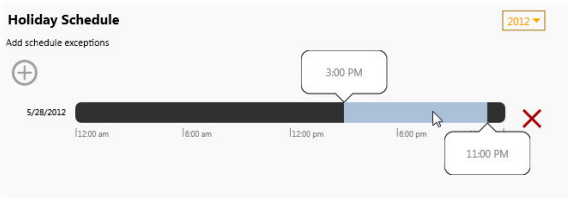


Figure 138 Setting a Time Range during a Holiday

7. Repeat steps 1-6 for each Holiday for this Distribution Group.

To Delete a Holiday Schedule

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Holiday Schedule** parameter for the group whose Holiday Schedule you wish to remove.

2. To delete a Time Range for a particular holiday, click on the range itself and click the **Remove** button in the resulting Time Range pop-up.

3. To delete an entire holiday day, click the Delete Holiday icon.

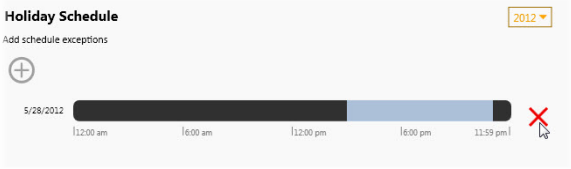


Figure 139 Delete a Holiday icon

The Holiday is removed from the schedule.

Logs Tab

The Logs Tab provides visibility into the activity Operators perform with Ocularis. Manual actions that someone performs are logged in a new database ('VSAudits'). Currently, the log tracks Ocularis Client usage. The 'admin' user as well as Group Administrators have visibility into this data. (Group Administrators may only view data related to their own group). By default, the audit log is disabled and administrators must enable it for activity to be logged.

Configure Auditing

Auditing is done system-wide and includes all users of Ocularis. Only the user 'admin' can configure the settings for the audit log. By default, the audit log is not enabled and only the user 'admin' can turn it on.

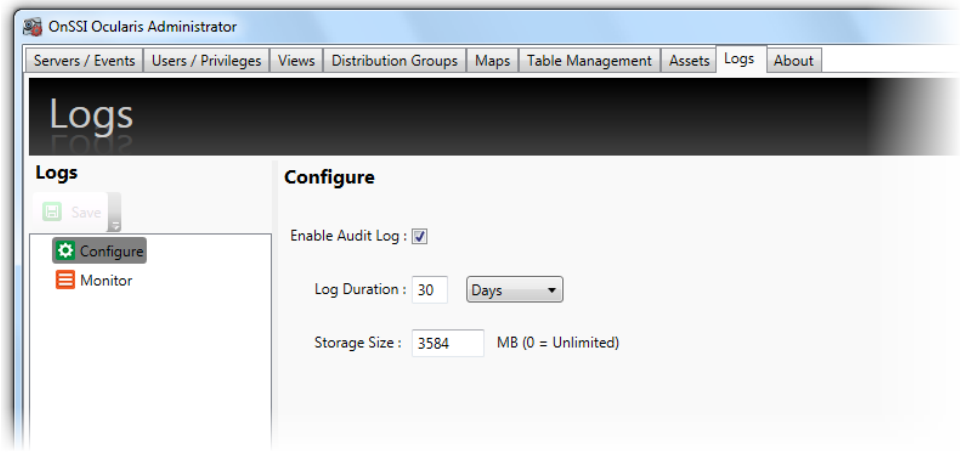


Figure 140 Configure the Audit Log

TO CONFIGURE AUDIT LOG SETTINGS

1. In the **Logs** Tab, select the **Configure** node.
2. Make changes to the **Configure** settings shown.
3. Click the **Save** button.

Field in the **Configure** pane include:

Enable Audit Log	This checkbox enables or disables system auditing. If the box is checked while Ocularis Client users are currently logged into Ocularis Base, actions performed by those logged in users will NOT be logged until their next session (the next time they log in to Ocularis). The default value is off/disabled.
Log Duration	Available units are: Hours, Days and Months. Log data will be retained for this period and purged once the duration has been reached.
Storage Size	This is the maximum size of the log database you want to dedicate for audit logging. The default value 3584 MB (or 3.5 GB) is well within the 4GB max limit for SQL Express. However, you can make the maximum database size any value you want, including 0 for unlimited size.

Storage of Log Data

As the system is used, each action is entered as one record into the log database, a separate SQL database within Ocularis. As you can imagine, this database can rapidly grow in size and fill up quickly. Data is written to the database in FIFO format ('first in, first out') so if the database is full, the oldest data is purged. Administrators have an option to control the size and/or the duration of maintaining data using the **Storage Size** and **Log Duration** settings respectively.

The log database is examined every hour. The **Storage Size** is checked first and the oldest data over the limit will be purged. Additionally, data that is older than the **Log Duration** setting will automatically be purged

What Data is Audited?

The data that is captured in the audit log is any action that a user performs manually in Ocularis Client. Automated actions, such as blank screen alerting, critical camera failover, etc. are not tracked in the audit log at this time. Anything that a user can 'click' is tracked. (See **Note*** below). Additionally, log-ins to Ocularis Administrator are also tracked.

***Note**:* *In Ocularis v4.0, the following user actions are NOT captured in the audit log:*

Maximizing a View Pane

Using controls on a video wall

Using controls on a map

Tools and functions within the Alert Manager

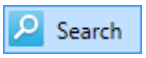
For additional limitations, please see the Ocularis Release Notes.

Note: *Actions performed in Ocularis Client v4.0 and later will be tracked in the audit log. While you can use earlier versions of Ocularis Client with Ocularis v4.0, the audit function is not supported.*

Viewing the Audit Log

Administrators can view entries of the audit log via the **Logs** tab in Ocularis Administrator. Group Administrators can view data from users within their own group and the user 'admin' can view all entries in the log. Search criteria are available to filter the log and an export function allows for the data to be exported and saved.

TO QUERY THE AUDIT LOG

1. In the **Logs** Tab, select the **Monitor** node.
2. Select any desired **Filter** criteria.
3. Click the **Search** button. 

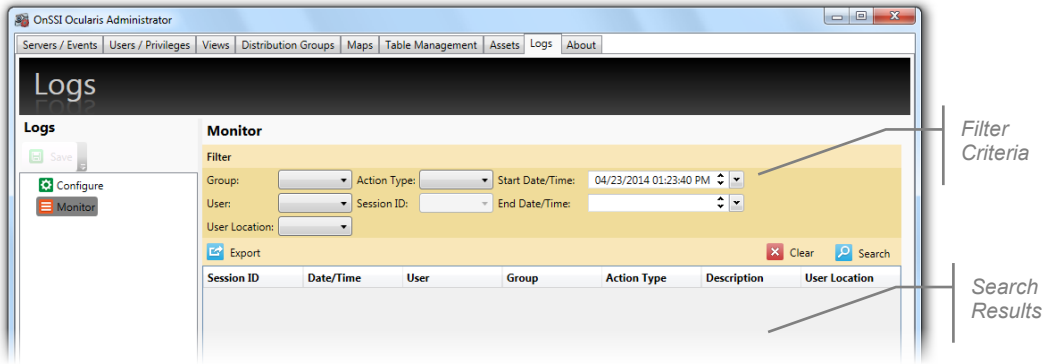


Figure 141 Logs Tab

The following fields are available for filtering the search results:

Group	This is the Ocularis user group.
User	This is the Ocularis User account.
User Location	This is the IP address of the Ocularis Client computer.
Action Type	This is the category related to the audited item. E.g. Authentication For more information, see Action Types below.
Session ID	Each time a user logs in to Ocularis Client, they are assigned a unique Session ID. This field can be used as filter criteria.
Start Date/Time	You can filter by the start date or start time of the records. The default value when you first enter the Logs tab is one hour prior to the current time.
End Date/Time	The end time by which you want to filter log data.

The drop-down lists for the above fields are dynamic based on the displayed results. For instance, if there are 5 users logged into the system but only 3 users have records for performing a Digital PTZ action, only those 3 user accounts will appear in the drop-down list as a filter option.

Note: *In Ocularis 4.0, you must close and re-login to Ocularis Administrator to refresh the data in the search criteria drop-down lists.*

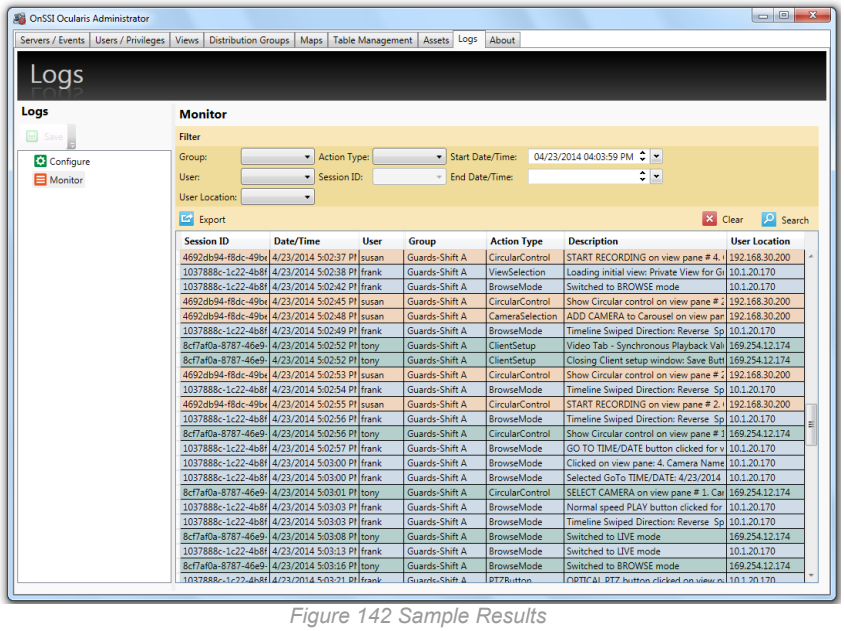


Figure 142 Sample Results

Action Types

Entries into the audit log are categorized into the following Action Types:

```
AuxButton
Authentication
BackwardButton
BrowseExport
BrowseMode
BrowseMotionDetection
BrowseTimeSlice
CameraSelection
CarouselNavigation
CircularControl
ClientSetup
DigitalPTZ
ForwardButton
Hotspot
MicrophoneButton
OpticalPTZ
PanamorphMode
PauseLiveVideo
PTZButton
SnapshotButton
SpeakerButton
StreamingInfo
ViewSelection
```

Search Results

Audit records are displayed in tabular format as shown in Figure 142. Results are displayed by default in order of *Date/Time*, most recent to oldest. Each Session ID has its own unique color to aid in reading the log.

Tool tip

If the column is not wide enough to display the associated data within the cell, position the mouse over the item to see an expanded tool tip of the cell contents.

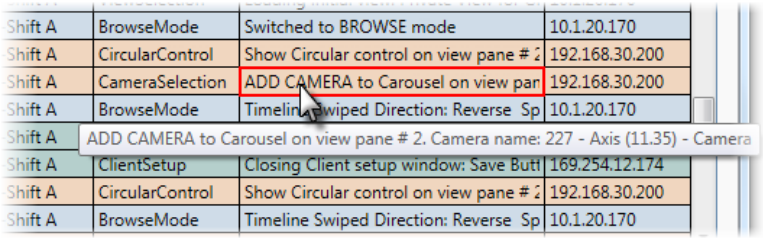

Shift A BrowseMode Switched to BROWSE mode 10.1.20.170
Shift A CircularControl Show Circular control on view pane # 2 192.168.30.200
Shift A CameraSelection ADD CAMERA to Carousel on view par 192.168.30.200
Shift A BrowseMode Timeline Swiped Direction: Reverse Sp 10.1.20.170
Shift A ADD CAMERA to Carousel on view pane # 2. Camera name: 227 - Axis (11.35) - Camera
Shift A ClientSetup Closing Client setup window: Save Butt 169.254.12.174
Shift A CircularControl Show Circular control on view pane # 2 192.168.30.200
Shift A BrowseMode Timeline Swiped Direction: Reverse Sp 10.1.20.170

Figure 143 Tool tip

Resize a Column

If you want to change the size of a column in order to better organize its contents, click and drag the column heading divider to resize that column.

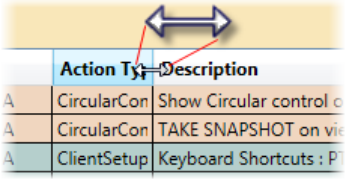


Figure 144 Resize a column

Reorder a Column

Click and drag a column heading along the row to reorder the table.

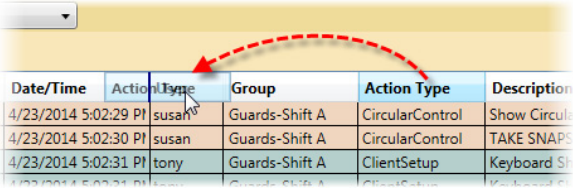


Figure 145 Reorder Columns

Re-sort a Column

By default, the records are listed in order of date/time where the oldest date/time record is at the top of the list. To sort the search results by any column, click on the column heading.

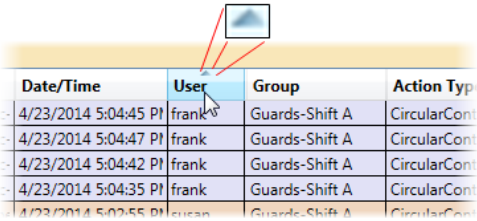
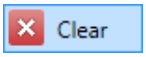


Figure 146 Sort any column

Click the same column again to reverse the sort order. The triangular sort icon will appear and indicate whether the sort is ascending or descending.

Clear Results

At any time, if you want to start over or simply clear the screen, click the **Clear** button. 

Session ID Search

Since Session ID is a large, complex identifier for each unique login session, a right-click option has been added. Right-click a Session ID on the results to see the following menu:

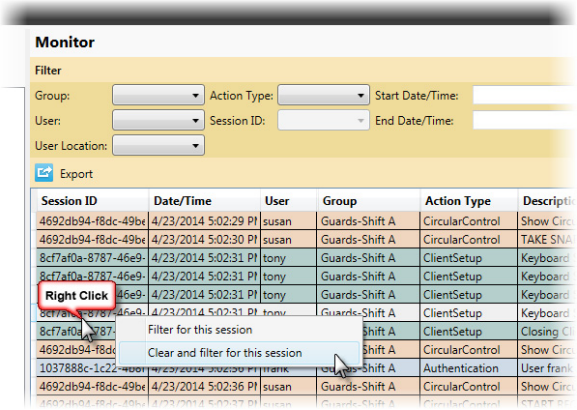


Figure 147 Right-click Session ID

- **Filter for this session** – this option will retain any filter criteria and add the selected Session ID as an additional filter. The new filters are immediately applied to the data.
- **Clear and filter for this session** – this option clears any filters already selected and queries the log with just the selected Session ID. The new filter is immediately applied to the data. This is equivalent to selecting the Session ID from the drop-down list.

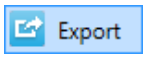
About Displayed Search Results

- Search results on the screen are by default sorted in descending order by *Date/Time* and limited to the newest (most recent) 5,000 records. If you want to access all records from the results of a search, you should **Export** the search results. (see *Exporting the Audit Log* on page 141)
- Changes made to the screen interface (resizing, re-sorting or reordering a column) are only temporary. The screen will revert back to default settings the next time the administrator logs in to Ocularis Administrator. These formatting changes will not be reflected in an exported .csv file.

Exporting the Audit Log

Audit Log search results may be exported to a .csv (comma separate value) file. This provides the administrator with the ability to use external tools (such as Microsoft Excel) to work with the log data. When search results are exported, all records of the query, regardless of size, are included.

TO EXPORT AUDIT LOG RESULTS

1. Query the log with the desired filters. (see *To Query the Audit Log* on page 136)
2. Click the **Export** button. 

The *Audit Log Export* screen appears.

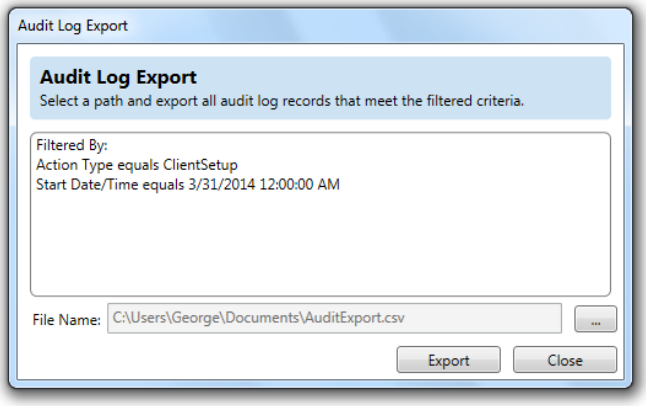


Figure 148 Audit Log Export pop-up

The pop-up identifies any criteria used as a filter. The default path and filename is presented:
`c:\Users\<PC Name>\Documents\AuditExport.csv`

3. To change the name or location of the exported file, click the ellipsis button.

4. Use standard Windows methods for choosing an alternate path and file name.
5. Click the **Save** button.
6. When the export is complete, a message '**Export Successful**' appears at the bottom of the pop-up.
7. Click **Close**.

Note: *The data exported is based on the filter criteria and will be inclusive of all records that meet the criteria.*

About Exported Search Results

- Search results on the screen are limited to the newest 5,000 records but if there are more records, these will all be included in an exported search.
- The order of the data in the .csv export is static. If you changed the order of columns in your audit log display, this order will not be reflected in the exported file. Use a third party application that supports .csv files to modify the column order.
- When you click the **Export** button, the query to the database is made again based on the criteria listed under 'Filtered By'. It does not simply export results you might have on the screen. The search results in an export include the most up-to-date results from the database at the time the user clicks the **Export** button. Therefore, these results may differ from those which may have been displayed on the screen due to the fact that the **Export** query was made after the initial **Search** query.

TO CANCEL AN EXPORT

Most exports occur within seconds. However, when you export data of a significant size it may take some time to complete the export. You are able to cancel an export while it is still in progress if necessary.

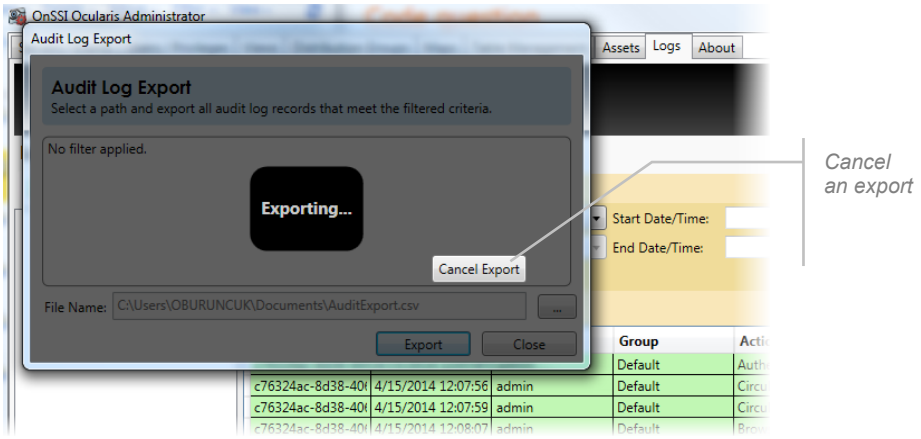


Figure 149 Cancel an Export

Click the **Cancel Export** button during the export process to cancel.

TO VIEW EXPORTED AUDIT LOG RESULTS

1. Use any third party application that supports .csv files to open the exported file that was created in step 5 above. The most common application to use is a spreadsheet application.

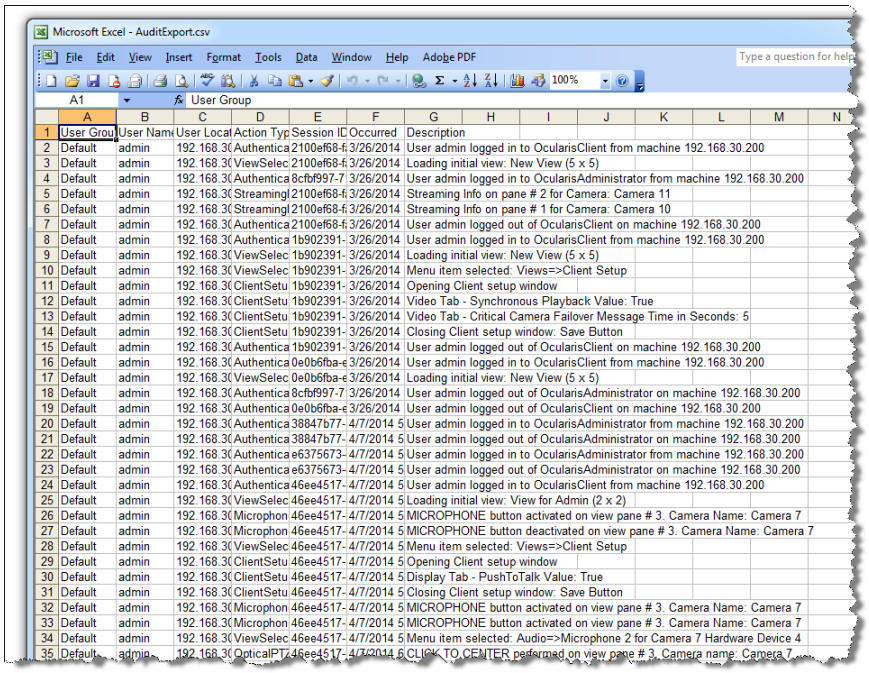

Microsoft Excel - AuditExport.csv
File Edit View Insert Format Tools Data Window Help Adobe PDF
A1 User Group
User Group | User Name | User Location | Action Type | Session ID | Occurred | Description
Default admin 192.168.30(Authentica 2100ef68-f 3/26/2014 User admin logged in to OcularisClient from machine 192.168.30.200
Default admin 192.168.30(ViewSelec 2100ef68-f 3/26/2014 Loading initial view: New View (5 x 5)
Default admin 192.168.30(Authentica 8cfbf997-7 3/26/2014 User admin logged in to OcularisAdministrator from machine 192.168.30.200
Default admin 192.168.30(Streaming 2100ef68-f 3/26/2014 Streaming Info on pane # 2 for Camera: Camera 11
Default admin 192.168.30(Streaming 2100ef68-f 3/26/2014 Streaming Info on pane # 1 for Camera: Camera 10
Default admin 192.168.30(Authentica 2100ef68-f 3/26/2014 User admin logged out of OcularisClient on machine 192.168.30.200
Default admin 192.168.30(Authentica 1b902391- 3/26/2014 User admin logged in to OcularisClient from machine 192.168.30.200
Default admin 192.168.30(ViewSelec 1b902391- 3/26/2014 Loading initial view: New View (5 x 5)
Default admin 192.168.30(ViewSelec 1b902391- 3/26/2014 Menu item selected: Views=>Client Setup
Default admin 192.168.30(ClientSetu 1b902391- 3/26/2014 Opening Client setup window
Default admin 192.168.30(ClientSetu 1b902391- 3/26/2014 Video Tab - Synchronous Playback Value: True
Default admin 192.168.30(ClientSetu 1b902391- 3/26/2014 Video Tab - Critical Camera Failover Message Time in Seconds: 5
Default admin 192.168.30(ClientSetu 1b902391- 3/26/2014 Closing Client setup window: Save Button
Default admin 192.168.30(Authentica 1b902391- 3/26/2014 User admin logged out of OcularisClient on machine 192.168.30.200
Default admin 192.168.30(Authentica 0e0b6fba-e 3/26/2014 User admin logged in to OcularisClient from machine 192.168.30.200
Default admin 192.168.30(ViewSelec 0e0b6fba-e 3/26/2014 Loading initial view: New View (5 x 5)
Default admin 192.168.30(Authentica 8cfbf997-7 3/26/2014 User admin logged out of OcularisAdministrator on machine 192.168.30.200
Default admin 192.168.30(Authentica 0e0b6fba-e 3/26/2014 User admin logged out of OcularisClient on machine 192.168.30.200
Default admin 192.168.30(Authentica 38847b77- 4/7/2014 5 User admin logged in to OcularisAdministrator from machine 192.168.30.200
Default admin 192.168.30(Authentica 38847b77- 4/7/2014 5 User admin logged out of OcularisAdministrator on machine 192.168.30.200
Default admin 192.168.30(Authentica e6375673- 4/7/2014 5 User admin logged in to OcularisAdministrator from machine 192.168.30.200
Default admin 192.168.30(Authentica e6375673- 4/7/2014 5 User admin logged out of OcularisAdministrator on machine 192.168.30.200
Default admin 192.168.30(Authentica 46ee4517- 4/7/2014 5 User admin logged in to OcularisClient from machine 192.168.30.200
Default admin 192.168.30(ViewSelec 46ee4517- 4/7/2014 5 Loading initial view: View for Admin (2 x 2)
Default admin 192.168.30(Microphon 46ee4517- 4/7/2014 5 MICROPHONE button activated on view pane # 3. Camera Name: Camera 7
Default admin 192.168.30(Microphon 46ee4517- 4/7/2014 5 MICROPHONE button deactivated on view pane # 3. Camera Name: Camera 7
Default admin 192.168.30(ViewSelec 46ee4517- 4/7/2014 5 Menu item selected: Views=>Client Setup
Default admin 192.168.30(ClientSetu 46ee4517- 4/7/2014 5 Opening Client setup window
Default admin 192.168.30(ClientSetu 46ee4517- 4/7/2014 5 Display Tab - PushToTalk Value: True
Default admin 192.168.30(ClientSetu 46ee4517- 4/7/2014 5 Closing Client setup window: Save Button
Default admin 192.168.30(Microphon 46ee4517- 4/7/2014 5 MICROPHONE button activated on view pane # 3. Camera Name: Camera 7
Default admin 192.168.30(Microphon 46ee4517- 4/7/2014 5 MICROPHONE button activated on view pane # 3. Camera Name: Camera 7
Default admin 192.168.30(ViewSelec 46ee4517- 4/7/2014 5 Menu item selected: Audio=>Microphone 2 for Camera 7 Hardware Device 4
Default admin 192.168.30(OpticalPT 46ee4517- 4/7/2014 5 CLICK TO CENTER performed on view pane # 3. Camera name: Camera 7

Figure 150Sample Exported Log as viewed in Excel

2. Use the third party application's tools to view, sort and print the data.

About Tab

The About Tab displays system information regarding the Ocularis installation. The display is divided into three sub-tabs:

- About Ocularis
- License Information
- Help

About Ocularis

The **About Ocularis** sub-tab displays version and build information for the Ocularis Administrator / Base installation.

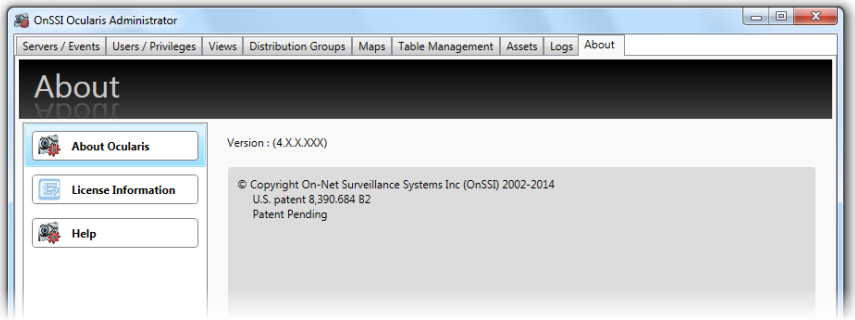


Figure 151 Version Information on the About Tab

License Information

The **License Information** sub-tab provides a unified display of Ocularis license information as well as the number of cameras used and their corresponding recording components.

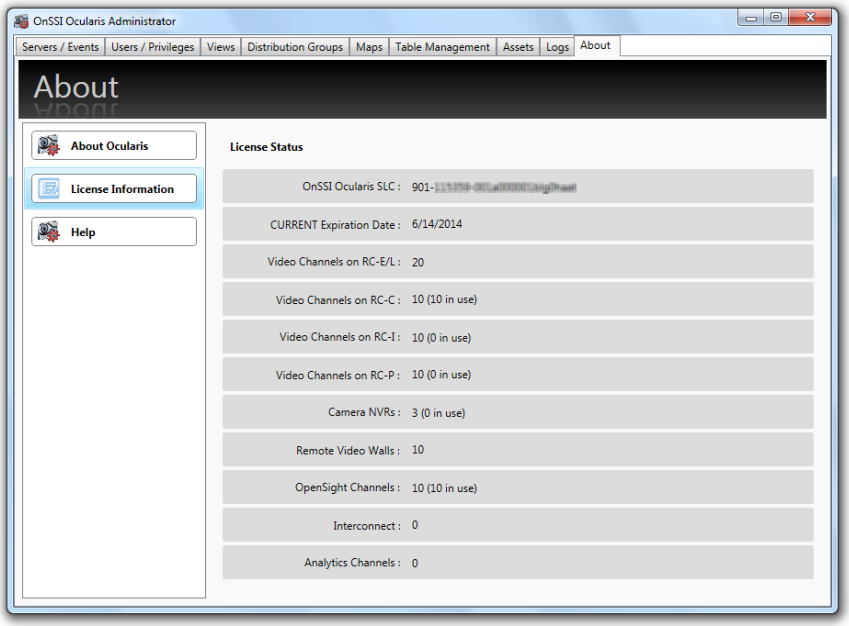


Figure 152 Ocularis Licensing Information

The number of licenses purchased is followed by the number in use. Video Channel licenses are assigned by the administrator in the **Servers / Events** tab. (See *Selecting Licensed Cameras* on page 15).

For Ocularis LS and Ocularis ES, the camera license total is combined and shown together on a single line.

Help

Click the **Help** sub-tab to launch the Ocularis Administrator User Manual using the corresponding PDF reader.

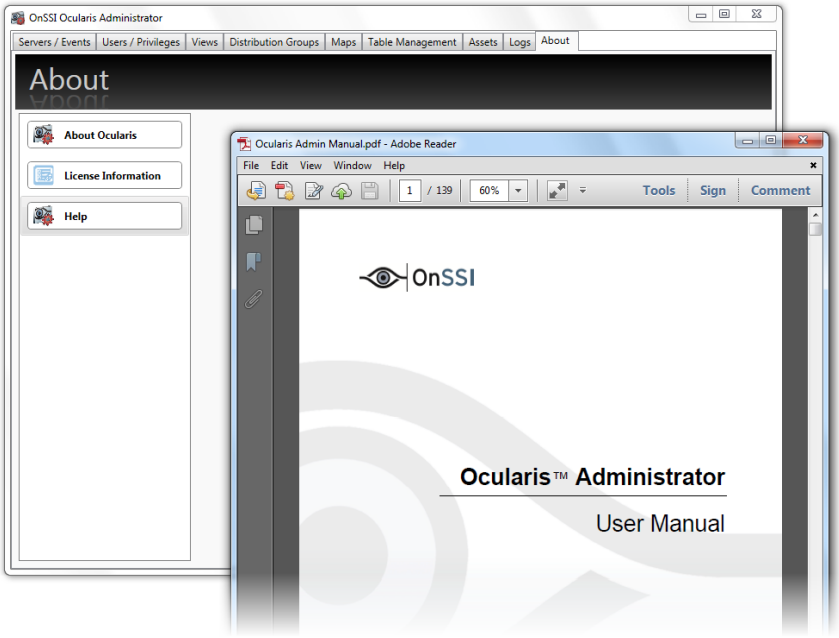


Figure 153 Launch Help File for Ocularis Administrator

Appendix

The following topics are discussed in this appendix:

- The OnSSI Event Coordinator

The OnSSI Event Coordinator

The OnSSI Event Coordinator is a service that does much more than coordinate events. It is responsible for the following:

- Storing incoming events in the Ocularis Base database
- Dispatching received events to subscribed clients
- Adding / Updating event sources from event proxies
- Generating thumbnail images from camera streams
- Exporting Bookmarks

The OnSSI Event Coordinator (OnSSI EC) works with Windows Message Queuing to receive events from the NVR Event Proxies, store them in the database and pass the events to the subscribed *Ocularis Client(s).* The OnSSI EC resides on the server where Ocularis Base is installed and it is installed automatically during Ocularis Base installation.

Some behavioral items to note if the OnSSI EC is stopped:

- You should still be able to log in to *Ocularis Administrator*
- You will be able to add and update NVRs
- The *Ocularis Administrator* Views tab will not display live thumbnail images of privileged cameras.
- The NVR event source, however, will not appear in the Events pane of the **Servers / Events** tab. Therefore, you will not be able to assign the event filter to a distribution group.
- The *Ocularis Client* user will not display the event counter in the upper left corner of the screen.
- The *Ocularis Client* user will not be able to display events in the Alerts Manager.
- The *Ocularis Client* user will be able to create a bookmark but will not be able to view it. Be sure that the OnSSI EC is running before creating a bookmark!

The OnSSI EC may be stopped, started or restarted from the Windows Services screen:

1. Right-click My Computer
2. Select Manage
3. Select Service and Applications
4. Select Services

The service is listed as: *OnSSI Event Coordinator Service*.

Contact Information

On-Net Surveillance Systems (OnSSI)

One Blue Plaza
7th Floor
P.O. Box 1555
Pearl River, NY 10965

Website:	www.onssi.com	
General:	info@onssi.com	845.732.7900
Fax:		845.732.7999
Sales Support:	sales@onssi.com	845.732.7900 x 1
PreSales Support	se@onssi.com	845.732.7900 x 2
Technical Support:	support@onssi.com	845.732.7900 x 3
Training:	training@onssi.com	845.732.7900 x 4
Marketing:	marketing@onssi.com	845.732.7900 x 5